8 The evolution of the Russian way of informatsionnaya voyna

Sean Ainsworth

Introduction

In recent years, numerous policy makers, military officials, and scholars have warned of the threat posed by a "new Russian way of war" (Thomas, 2016; Seely, 2017) which blends a range of means, including both kinetic and non-kinetic, military and non-military, as well as overt and covert. This "new way of war" has been employed in efforts to assert regional hegemony and dominance over what Russia regards as the "near abroad" of former Soviet republics and to project Russian power to defend Russian interests further afield, such as in Syria.

One of the core components of the "new way of war" is Russia's exploitation of emerging technologies, employing information-technology systems and networks for coercive purposes. In recent years, Russia has grown increasingly bold, engaging in cyber and information warfare operations, targeting the democratic processes and systems of several Western states, and bringing the specter of Russian cyber and information warfare to the fore of Western strategic thought (Greenberg, 2017; Office of the Director of National Intelligence, 2017; Saeed, 2017).

However, this is not an entirely new phenomenon or way of war. Russia's cyber and information warfare operations have been informed and shaped by its experiences in post–Soviet conflicts in addition to Moscow's strategic understanding of the West's actions, motivations, and Russia's newfound place in the post–Cold War international system. These experiences have driven Russia to adapt Soviet-era military doctrine and geopolitical strategies to take advantage of the virtual strategic environment created by the information revolution and emerging technologies.

This chapter first explores the historical foundations and precedent of Russia's strategic thought and doctrine concerning information warfare. It then examines the factors that have motivated Russia's adaptation of these earlier theories to the new fifth domain of war – cyberspace. This includes a consideration of Russia's experiences during the wars in Chechnya and concern over Western influence and interference within the near abroad of former Soviet satellites. The chapter analyzes how these adaptations have been actively employed by Russia in the pursuit of its interests in the near abroad, including Estonia, Lithuania, Georgia, and

Ukraine. Finally, the chapter discusses the potential future capabilities of artificial intelligence (AI)-enabled information warfare.

Russian doctrine and strategic thought

The development of military doctrine and strategy is shaped by a state's unique historical, cultural, and political background. As a result, there are substantial differences between Western military conceptualizations of the role of emerging technologies and means or domains of conflict, such as cyberspace, and how they are understood within Russian military doctrine and strategic thought.

Russia's strategic military theorists, for example, tend to use terms such as "cyberwarfare" only when translating and discussing Western strategic thought and doctrine (Giles and Hagestad, 2013). Similarly, Russian strategic thought refers to the "information space" (*informatsionnye prostranstvo*) rather than "cyberspace", the term commonly used in the West. While seemingly similar, these concepts are, in fact, substantially different from one another with implications for the ability of states to understand and predict Russian strategy and military actions. Western definitions of cyberspace tend to focus on the hardware and infrastructure; both the US military and North Atlantic Treaty Organization (NATO) define cyberspace as a global domain of interconnected technology and communications infrastructure, including telecommunications networks and computer systems (US Joint Chiefs of Staff, 2018, p. GL-4; NATO Standardization Office, 2019). The focus on the infrastructural hardware establishes the boundaries of Western approaches to cyberwarfare as offensive cyber operations designed to deny, degrade, disrupt, or destroy an adversary's cyberspace assets and capabilities. The Russian information space concept, by contrast, extends this definition to also include human cognitive domains and social consciousness elements (Ministry of Defence of the Russian Federation, 2011, p. 5). This is a significant definitional difference, affecting Russian and Western strategic thought and understanding concerning the role of offensive cyber operations. For example, Western militaries tend to delineate between cyberwarfare, information operations, and psychological warfare as separate, though closely related, and often interdependent tools in the toolkit. Russia instead views all three as falling within a broad overall concept of "information war" (*informatsionnaya voyna*), which is a continuous ongoing confrontation not necessarily limited to wartime (Giles, 2016, p. 4). Within this concept, Russian military theorists do recognize a division between "information-technical" and "information-psychological" means, which roughly align with Western conceptualizations of "cyberwarfare" and "information warfare" respectively (ibid, p. 9).

Russia's more comprehensive information warfare concept is arguably a continuation of long-running Russian strategic thought and historical military doctrines that have been adapted to the cyber domain. These adaptations have been driven by both internal and external factors and strategic threats or possibilities that have emerged alongside the technologies of the information revolution. In the mid-1990s, as Russia was adjusting to its substantially weakened military position

following the dissolution of the Soviet Union, Russian military theorists began to emphasize the growing role of non-kinetic means of projecting power, most importantly those relating to the ongoing information revolution (Blank, 2013, p. 34; Gerasimov, 2016). The value of these methods was that they depended on means other than the use of raw military power or kinetic force during a period when the Russian military was declining, and it was preparing for, and undertaking, substantial modernization and reform. Indeed, the Russian military has long emphasized the importance of the informational domain of conflict in an effort to overcome its own economic or military weaknesses. Russian information warfare stems from the adaptation and application of several historical Russian strategies to the cyber domain, most notably the Soviet-era military doctrine of *maskirovka* (typically translated as camouflage or deception). Emphasizing the strategic importance of operational concealment and deception, *maskirovka* comprised "a set of processes … designed to mislead, confuse, and interfere with anyone accurately assessing [the Soviet Union's] plans, objectives, strengths, and weaknesses" (Shea, 2002, p. 63).

Maskirovka is therefore closely aligned with Soviet intelligence services employment of "active measures" to coerce and subvert during the Cold War, in addition to the Soviet military strategy of "reflexive control". Reflexive control forms a critical component of Russian information warfare. The author of the theory and a key figure in its development under the Soviet military, Vladimir Lefebvre, defines reflexive control as "conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision" (cited in Chotikul, 1986, p. 5). In essence, reflexive control is the creation of a reality that leads the target to make a decision of their own "free will" that benefits the controller, akin to a chess player baiting their opponent into exposing their queen. Reflexive control formed "an integral, valuable, and potentially very lethal part of the Soviet decision making process" (Chotikul, 1986, p. 90), though some Western analysts expressed doubts regarding its efficacy due to the "impossibility of reducing thought processes and psychological functioning to quantitative, exact objects of control" (ibid, p. 96).

As this chapter demonstrates, the technological developments of the information revolution and the emergence of a "global village" connected through cyberspace has created opportunities for the identification and exploitation of thought processes and psychological functioning as specific "objects" of control. The tracking and data harvesting conducted by social media websites and other online services has enabled information warfare operations to target audiences with unprecedented specificity: Audiences are now able to be targeted with precision based on specific characteristics including political leanings, geographic location, age, gender, and occupation. Similarly, by exploiting the algorithms that select which content is recommended or displayed to a user, information warfare operations can attach themselves to, or blend into, popular topics and categories of content. User engagement with the inserted material leads the algorithm to recommend more material from the same source or of a similar nature. This is a strategy that has been employed by Russian state broadcaster Russia Today (RT) on

YouTube, achieving user engagement through the upload of non-political "click-bait" videos in the hope that the algorithm recommends additional content with a political focus (EU East Stratcom Task Force, 2017). As such, users' choices are structured for them without their knowledge.

Reflexive control in the informatsionnye prostranstvo

Despite the historical precedent and interest of the Russian state in the mid-1990s to innovate in the information domain owing to its declining material hard power, it was not until the early 2000s that these methods came to the fore of Russian strategic thought. The primary driving factors for this adjustment were the political and military failings Russia experienced during the First Chechen War, in addition to Russia's strategic understanding of the "Color Revolutions", which it saw as a series of connected pro-Western democratic protest movements throughout the near abroad (Cordesman, 2014).

The Chechen Wars

The First Chechen War (1994–1996) exposed substantial failings in Russia's military doctrine, organizational structure, and strategy. It also demonstrated the potential power of the emerging information domain because of the technological developments of the information revolution. In December 1994, tensions between Moscow and the breakaway republic of Chechnya escalated, leading to a brutal 20-month long conflict which resulted in a Russian defeat despite the Russian military's overwhelming advantage in the numbers of available manpower, armored vehicles, firepower, and air support. A substantial contributory factor in Russia's defeat was undoubtedly its reliance on Cold War–era military doctrine designed to fight a peer–competitor, with a substantial focus on mass troop and armored vehicle movements, coupled with the use of devastating supportive fire and aerial bombardment (Arquilla and Karasik, 1999). This approach was ill-suited to combatting the networked and decentralized Chechen separatists, who typically fought in highly mobile bands of 12–20 fighters capable of rapidly swarming and overwhelming Russian forces.

The exploitation of the information space in the conflict was, arguably, more consequential for a Chechen victory than kinetic military operations. Facing an overwhelmingly militarily superior opponent, the Chechen separatists, many of whom were former members of the Soviet military, recognized the military value of the informational-psychological domain of the conflict. The separatists concentrated their information warfare efforts along two lines: First, engendering sympathy and support from the international community, and second, fomenting disillusionment and harming the morale of Russian troops and the Russian public. The separatists created websites and online communities targeting the Chechen diaspora and international non-governmental organizations (NGOs). This provided a direct means of distributing the Chechen narrative, distributing images and video of civilian casualties caused by Russian bombardments as

part of a wider effort to portray Chechens as helpless victims of Russian cruelty. These efforts rallied international support for the legitimacy of Chechen separatism and condemnation of Russia (Fayutkin, 2006). Whereas Chechen separatists welcomed journalists and cooperated with media filming and photography, the Russian military's lack of cooperation with, and hostility toward, the media prevented any potential counter-narrative from emerging.

The combined effects of a lack of effective military and political leadership, the brutality of the conflict, and Chechen information warfare proved devastating for the morale of Russian troops (Arquilla and Karasik, 1999, p. 221). Chechen radio broadcasts would address Russian officers by name, listing the names and location of their wives and children, and claiming that they were targets of Chechen "hit-squads" (Arquilla and Karasik, 1999, p. 217). The breakdown in the morale of Russian forces proved of substantial benefit during the Third Battle of Grozny, when Chechen separatists, who were outnumbered approximately eight to one, were able to retake the Chechen capital and force the surrender of approximately 7,000 Russian troops stationed in the city. Information warfare targeting the wider Russian public included "pirate" television and radio broadcasts, in addition to the use of radio-jamming equipment to prevent Russian broadcasts within Chechnya (Arquilla and Karasik, 1999). Taking advantage of public suspicion that the war was a political distraction by the beleaguered Yeltsin government, the separatists were able to substantially undermine the Russian public's support for the war effort. These efforts created the political impetus for a negotiated solution to the conflict, which was only hastened by the success of separatist forces during the Third Battle of Grozny.

Official Russian assessments of the conflict focused on the advantage the separatists gained through their employment of information warfare. Sergei Stepashin, then Director of the Federal Security Service until his resignation following a Chechen terrorist attack in June 1995, later noted that "the information war was lost" (Arquilla and Karasik, 1999, p. 217). Similarly, Dan Fayutkin, the head of the Israeli Defense Force's Doctrine Section, suggests that the conflict "teaches us the importance of information warfare in the realization of political and military goals" (Fayutkin, 2006, p. 55) and that "it was consistent, well-thought-out, and potent propaganda" (ibid) that ensured Chechen victory. Indeed, the war was regarded as a crisis point for the Russian military's public communications systems and state media organizations (Sieca-Kozlowski, 2009, p. 304). In this way, the First Chechen War not only provided the impetus for much-needed Russian military reform; it also served as an early lesson regarding the value and necessity of harnessing the new strategic informational environment created by cyberspace and the growing role that information dominance would play in future conflicts.

Russian military and security services, bruised by the failure to counter Chechen use of information warfare, adapted relatively quickly in the three years interim before the start of the Second Chechen War (1999–2009). Russia recognized the effectiveness of the separatists' exploitation of Russian mass media during the First Chechen War for information warfare purposes, including strategic messaging, damaging troop morale, and weakening public support. As a

result, Russia established new censorship regimes and the Russian Information Center (*Rosinformtsentr*). Managed by the Russian Army, the Center was ostensibly intended to filter the flow of information from the conflict zone in Chechnya to prevent the spread of disinformation and Chechen propaganda. In practice, the Center controlled and restricted Russian and foreign media access to information regarding the conflict that could prove damaging to the Russian government. The Center also distributed foreign press articles and material that were supportive of the Russian government's narrative to the Russian press for domestic distribution (Sieca-Kozlowski, 2009, p. 305). Announcing the creation of the Center, Vladimir Putin, then-Prime Minister of Russia, remarked that Russia had "surrendered this terrain some time ago and now we are entering the game again" (Dixon, 1999). These reforms proved decisive in securing, and maintaining, public support for the war effort by restricting Chechen messaging efforts, limiting media reporting to the official government narrative, and insulating the Russian information space from the escalating levels of violence and rising casualties during the prolonged insurgency (Pain, 2000; Thomas, 2003).

Lessons learned from the Chechen wars were incorporated into Russia's 2000 *Information Security Doctrine*. The doctrine outlines a range of threats to Russia's information space and necessary future policy approaches. One of the major internal threats identified by the doctrine was the insufficient levels of coordination between various governmental bodies "in shaping and carrying out a unified state policy in the realm of national information security" (Russian Federation, 2000, p. 7). Other internal threats included insufficient levels of control over the Russian information space coupled with insufficiencies in government messaging efforts (Russian Federation, 2000, p. 8). In line with these identified threats and the 2000 *Russian Military Doctrine*, the *Information Security Doctrine* outlined several urgent measures, including "protecting society against distorted and untrustworthy information" (Russian Federation, 2000, p. 27) and "counteracting information war threats in a comprehensive way" (ibid, p. 29).

The Color Revolutions

These identified threats and countermeasures rapidly grew in importance following the Color Revolutions of the early 2000s, which arguably proved just as significant for the development of Russian strategic thought as the conflict in Chechnya. Presaged by the 2000 "Bulldozer Revolution" and overthrow of Slobodan Milošević in Serbia, the Color Revolutions were a series of pro-democratic youth and civic protests movements that took place throughout the near abroad of former Soviet satellites. The revolutions were able to achieve relatively rapid pro-Western regime change, beginning with the 2003 Rose Revolution in Georgia and extending to include the 2004 Orange Revolution in Ukraine and Kyrgyzstan's 2005 Tulip Revolution. Youth activists critical of the current regimes in these countries took advantage of the spread of new technologies, including internet access and text messaging, to communicate with one another and to circumvent government surveillance and censorship efforts. Internet access

and text messaging proved vital for communicating with other activist movements in neighboring countries in addition to international democracy promotion and human rights NGOs (Stent, 2014, pp. 100–102). Using the newly accessible technologies of the information revolution, activists were able to bypass the traditional barriers and restrictions of the existing information space and media environment to provide an alternative critical viewpoint and to attract the attention and support of foreign NGOs and governments (Stent, 2014).

In line with the 2000 *Information Security* and *Russian Military Doctrines*, a consensus view was reached within Russia that these revolutions formed a component of Western information warfare intended to undermine Russia's strategic position within the near abroad (Giles, 2019). Russia's foremost military theorist General Makhmut Gareev, for example, extended Russian suspicion of Western interference and malign machinations to include the collapse of the Soviet Union and Yugoslavia. Gareev described such threats as "assuming not so much military forms as direct or indirect forms of political, diplomatic, economic, and informational pressure, subversive activities, and interference in internal affairs" (Jonsson and Seely, 2015, p. 8). Similarly, in May 2005, Sergei Markov, a Russian political scientist and politician, accused Ukrainian protestors of having been paid $10 a day to protest by the US Central Intelligence Agency (Stent, 2014, p. 115).

This siege mentality and view of the Color Revolutions as a strategic threat to Russian national interests was wholly consistent with the 2000 *Information Security* and *Russian Military Doctrines*. It also aligns with the prevailing view concerning the collapse of the Soviet Union amongst the *siloviki* (former members of Soviet and Russian security services) members of the Russian leadership. Foremost among these *siloviki*, President Vladimir Putin in 2005 lamented the collapse of the Soviet Union as the 20th century's "greatest geopolitical catastrophe" (BBC News, 2005). In the Russian view, the regime changes achieved by the Color Revolutions were heightened by the strategic threat posed by the 1999 and 2004 rounds of NATO enlargement, as the new leadership in Georgia and Ukraine favored pursuing NATO membership (Oliker et al, 2015).

In the Russian leadership's view, the Color Revolutions were a component of Western information warfare intended to isolate and undermine Russia's strategic interests within the region. The Russian leadership therefore adopted a genuine fear that the West would soon extend this information warfare to Russia itself (Duncan, 2013). This siege mentality and growing suspicion is evident in Russia's 2014 *Military Doctrine*, which highlights the enlargement of NATO and stationing of military assets within NATO member-states that border Russia as the principal security threat facing Russia. Other identified threats include the use of information warfare to subvert the sovereignty, political independence, and territorial integrity of states to destabilize individual states and regions, in addition to the use of regime change to establish regimes in contiguous neighboring states with policies that threaten Russian interests (Russian Federation, 2014). Indeed, the oft-cited "Gerasimov Doctrine", stemming from a speech given by the Russian Army's Chief of the General Staff, Valery Gerasimov, was intended as a description not of a new Russian way of war but the supposed information

warfare targeting Russia carried out by the US and other Western states (Bartles, 2016; Galeotti, 2018).

The exploitation of the information revolution and new technologies

It was therefore defensive concerns that initially motivated Russia's adoption of an aggressive offensive information warfare strategy. Defeat in the First Chechen War, and ongoing instability in the Caucasus, posed a threat to Russia's territorial integrity, while Western influence and potential machinations targeting the near abroad threatened Russia's dominion over its historical sphere of influence. Russia's declining military hard power and the asymmetry of the post–Cold War balance of power heightened Moscow's perception of its vulnerability to that of an existential threat (Giles, 2016, pp. 36–41).

Viewing wholly defensive measures as too risky in the face of these combined threats, Russia adopted a strategy entailing the opportunistic employment of offensive information warfare. Indeed, in 2007 then-Defense Minister Sergei Ivanov remarked that "information itself [has turned] into a certain kind of weapon… that allows us to carry out would-be military actions in practically [a] theater of war and most importantly, without using military power" (Blank, 2013, p. 34). The foundational element of Russia's information warfare strategy is the employment of disinformation and misinformation-based propaganda.

Traditional propaganda methods, such as those pursued by both superpowers during the Cold War, are typically intended to persuade the reader or listener that the propagandists' objectives, system of government, or ideology are superior and more worthy of support. As such, traditional propaganda tends to emphasize factors such as "trust, credibility, actions, legitimacy, and reputations [which] are critical to success" (Defense Science Board, 2008, p. 39). By contrast, Russian information warfare strategies rely on what a 2016 RAND report described as the "firehose of falsehood" model (Paul and Matthews, 2016). Unlike traditional propaganda methods, the firehose of falsehood eschews any commitment to consistency or even an objective reality. Counterintuitively, the strategy actively incorporates these inconsistent and incredulous aspects into its strategic framework, exploiting inherent cognitive biases through the dissemination of rapid, continuous, and repetitive messaging across multiple channels of communication.

Contemporary Russian information warfare is not intended to portray Russia as superior to the West, but instead to "confuse, befuddle, and distract" (Lucas and Nimmo, 2015) while exploiting divisive social, political, and cultural issues to foster political polarization and division within targeted states. In recent years, many of the targeted states have included Western democracies (US Department of Homeland Security, 2016; Greenberg, 2017; Office of the Director of National Intelligence, 2017). However, of far more strategic importance for Russia are its information warfare campaigns targeting states within the near abroad.

Russian information warfare campaigns targeting the near abroad take the form of opportunistic reflexive control, with a specific focus on the fomenting

of political and ethnic tensions. The legacy of Soviet-era "russification" policies has resulted in substantial ethnic Russian minority populations throughout the near abroad. Official Russian policy refers to these diasporas as "compatriots", and a substantial number of Russian-language state media outlets are marketed toward the diasporic populations throughout the near abroad. As discussed above, rather than attempting to engineer political outcomes wholesale, Russia employs these media outlets to instigate and exacerbate divisions between ethnic Russian diasporas and the majority populations of targeted states through the "firehose of falsehoods" propaganda model. Russia's information warfare therefore follows an opportunistic strategy, using political and ethnic divisions to create seemingly "organic" political crises that can then be quickly escalated or subdued in accordance with Russia's interests at the time.

Russia's information warfare in Estonia, Lithuania, Georgia, and Ukraine

In 2007 a political dispute ensued between Russia and Estonia in response to the relocation of a Soviet-era war memorial. By leveraging its information warfare capabilities Russia was able to escalate the dispute into the worst civil unrest Estonia had experienced since the Soviet occupation. Estonian security services suspected the resultant riots were actively orchestrated by Russian intelligence and Special Forces (Cavegn, 2017). Russian state media outlets targeting the ethnic Russian diaspora in Estonia were broadcasting hyper-emotional coverage of the relocation, including false reports of police brutality and portrayals of ethnic Russians as facing a threat from Estonian fascists, to foster outrage amongst the ethnic Russian diaspora. Estonia also found itself the target of a substantial cyber-attack described by then-Estonian Defense Minister Jaak Aavisoo as affecting "the majority of the Estonian population", with "all major commercial banks, telcos, media outlets, and name servers… [feeling] the impact" (Davis, 2007). The attacks, in effect, placed Estonia under a "cyber siege" which lasted three weeks and was only halted by the Estonian government blocking all foreign internet traffic. The technological advances that had until that point been regarded as Estonia's comparative advantage were now a potential source of vulnerability. Several organizations and individuals have since claimed credit for the cyber-attacks, most notably *Nashi*, a Kremlin-linked youth movement. *Nashi* have previously been accused of and implicated in similar activities within Russia against adversaries of the Kremlin, including cyber-attacks targeting media organizations critical of Putin and the Kremlin. While it is possible that the cyber-attacks were carried out by patriotic hacker militias or criminal organizations, the suggestion that the attacks were not coordinated or at least tacitly sanctioned by the Kremlin stretches credulity. Even without any coordination, Russian state media coverage's purposefully emotional misinformation would have most likely served as the catalyst for any decision to attack Estonia by patriotic hacker militias.

By contrast, a similar legislative initiative by Lithuania in 2008 banned the public display of both Nazi and Soviet symbols, including images of Nazi and Soviet

leaders, flags, and insignia. This outraged many ethnic Russians, who viewed the law as equating the Soviet Union with Nazi Germany. In response, hundreds of Lithuanian websites were defaced by outraged "patriotic hacker" groups that called for an organized hacking campaign similar to the one that targeted Estonia, with the intention of including other Baltic states as well as Ukraine as targets (Danchev, 2008). However, in this instance, the patriotic hackers were either unwilling or incapable of escalating their attacks, with no organized campaign materializing. The inability to escalate the attacks from low-level "cyber-vandalism", despite enthusiasm from at least some patriotic hacker groups, would suggest that there was little widespread support to do so despite the similarities with Estonia the previous year. Alternatively, an escalation of the dispute may have been viewed as undesirable for Russia's interests. Indeed, there was little to no focus on the legislation by Russia's state media, much less the overly emotional disinformation that occurred in Estonia the previous year. One potential explanation for this lack of media coverage is the disparity in potential audience size: Ethnic Russians comprise 24% of Estonia's population, but total only approximately five percent of Lithuania's population, thereby limiting any opportunity to sow ethnic and political divisions.

Similar methods can be seen in the 2008 August War between Georgia and Russia, provoked by Georgia's aspirations for NATO membership (Kishkovsky, 2008). Russian information warfare portrayed Georgian responses to escalating attacks by South Ossetian separatists as acts of Georgian aggression against Russian compatriots. Russian state media organizations stationed journalists in South Ossetia days in advance of the conflict. When the war began, Russia's state news channels immediately displayed detailed graphics of the ongoing military operations as well as coordinated talking points accusing Georgia of genocide and ethnic cleansing (Whitmore, 2008).

The Russian military's counter-offensive became the first instance of the use of cyber operations in a combined operation with conventional military forces (Hollis, 2011). Georgian government networks were targeted by both cyber and kinetic attacks to disrupt government and military communications capabilities. Civilian communication networks near military areas of operation were also targeted as part of the cyber operation in order to foster panic and confusion amongst the civilian population (Haddick, 2011). These attacks disrupted the Georgian government's capability to communicate with the international community, reducing its ability to counter Russian narratives of the conflict. In an example of reflexive control through information warfare, the numerous conflicting narratives regarding the onset and conduct of the conflict led to widespread confusion within the international community and media (Fawn and Nalbandov, 2012). As a result, Russian information warfare was able to turn a traditional strength of NATO, its large membership, into a weakness. With so many members, the conflicting narratives generated by Russian information warfare stymied any potential for a cohesive international response. This left Western leaders reliant on urging restraint and attempting to negotiate ceasefires, thereby "ultimately tolerating the Russian fait accompli" (Socor, 2008).

Russia refined this synergistic combination of reflexive control and information warfare further still by the 2014 Euromaidan Revolution (also known as the Ukrainian Revolution). As in Georgia, Russia's information was founded in the prevailing Russian view of the Euromaidan protests as a continuation of Western-orchestrated Color Revolutions and a fear of Ukraine's aspirations toward NATO and EU membership. Russian state media presented the Euromaidan Revolution as a fascist coup orchestrated by the CIA, or Ukrainian "Nazis", that threatened the safety of Ukraine's ethnic Russian population and the Black Sea Fleet (Chalupa, 2014). Similar narratives were employed by Russian-financed "web brigades" on social media websites (Sindelar, 2014). These web brigade efforts included social media influence campaigns such as "Polite People", which "promoted the invasion of Crimea with pictures of Russian troops posing alongside girls, the elderly, and cats" (Seddon, 2014). At the same time, Russian government officials provided contradictory narratives and denials of objective fact (*maskirovka*). This brazen disregard for fact gave rise to the "little green men" phenomenon, as Russia continued to resolutely deny any military presence in Ukraine, even as it secured the annexation of the Crimean Peninsula. Western media organizations were unsure how to respond to Russia's strident denials in the face of objective reality, providing a window of opportunity for Russian state media organizations to push the Kremlin's narratives.

Russia attempted to buttress its information warfare portrayal of Euromaidan protesters as fascists by actively manipulating the published results of the 2014 Ukrainian presidential election. Malware was inserted by "CyberBerkut", a group the UK National Cyber Security Center asserts is a Russian military intelligence operation (GCHQ National Cyber Security Centre, 2018). CyberBerkut inserted malware onto the servers of Ukraine's electoral commission programmed to replace the official results page with an identical one that displayed the anti-Russian far-right candidate Dmytro Yarosh as the winner of the election. The malware was programmed to activate after the polls had closed but was discovered and removed by a Ukrainian cybersecurity company minutes beforehand. Despite this, Channel One Russia, a state media outlet, nonetheless reported Dmytro Yarosh as the winner, displaying a graphic of the false results page and citing the electoral commission's website, despite the manipulation and publication of false results having been prevented (Kramer and Higgins, 2017). Russia's annexation of Crimea involved simultaneous cyber-attacks targeting Ukraine's telecommunications infrastructure to disrupt the availability or flow of information to and from the peninsula. Russia's efforts to ensure regional information dominance and control, while confusing and delaying the international community's response, provides an excellent example of Russia's blending of reflexive control theory with contemporary information warfare. Because of these measures, Russia was able to secure the annexation of the peninsula through *fait accompli* in largely the same manner as it secured the de facto sovereignty of Georgia's breakaway regions, South Ossetia and Abkhazia, in the 2008 August War.

Future capabilities

The Kremlin views the development of AI technologies as a matter of strategic importance, encapsulated by President Vladimir Putin's claim that "whoever leads in AI will rule the world" (RT, 2017). As such, the Russian military has grown increasingly interested in the potential military application of AI technologies. This manifested in 2019 when the Kremlin outlined an ambitious national AI strategy primarily focused on supporting domestic research and development of AI and related technologies while preventing, or at least limiting, any dependence on foreign technologies (Office of the President of the Russian Federation, 2019). To date, most of the official discussions and demonstrations of military AI capabilities have focused on potential battlefield applications, such as AI-enabled combat and sensor systems. However, AI technologies may prove most effective, at least in the short-term future, in augmenting and enhancing Russia's information warfare strategies.

Russia's information warfare remains reliant on a significant amount of human labor, much of which is drawn from "troll farm" web-brigades-for-hire, where workers are expected to rapidly produce content, including managing multiple different social media accounts and making hundreds of posts or comments a day (Seddon, 2014). Some of these activities can be automated using simple social media bot software. However, such bot accounts are relatively simple for social media websites to detect and deactivate. Future bot accounts harnessing these AI technologies may not be so easy to counter, employing AI-generated synthesized portraits and photography to appear as a real person. The addition of text generation capable of mimicking human communication and behavioral patterns could theoretically enable such bot accounts to pose as real human beings to the extent that they are able to respond in real time and engage in conversations with other social media users.

Moreover, emerging AI technologies harnessing neural networks can generate increasingly sophisticated, difficult to detect, and hyper-realistic synthesized photo, video, and audio. The most notable example of this being "deepfake" artificial videos, wherein an individual may be depicted performing actions or taking part in an event that never took place. Similarly, ASI Data Science, an AI development company, developed an algorithm capable of producing a convincing recording of US President Donald Trump declaring a nuclear war against Russia using just two hours of source audio processed over five days (Chertoff and Rasmussen, 2019).

Conclusion

The development of Russia's cyber and information operations provides a startling example of the potential threats that can be created by new and emerging technologies. These threats can be particularly pernicious when emerging technologies are combined with unforeseen and innovative strategies designed to exploit fundamental weaknesses in their design and even human nature itself, as

in Russia's "firehose of falsehood" model. Despite the unconventional approach adopted by Russian information warfare, these "new tools" are ultimately founded in a long tradition of Russian military strategic thought, including *maskirovka* and reflexive control theory. Their development has, however, been shaped by dominant Russian strategic thought and narratives regarding supposed Western machinations intended to isolate Russia and the opportunistic exploitation of vulnerabilities created by new technological developments.

Russia's successful use of an evolving information warfare strategy throughout the near abroad stands in stark contrast to the failings experienced during the First Chechen War and likely influenced Russia's decision to engage in information warfare campaigns targeting Western democracies themselves. Through the exploitation of state media organizations and social media, Russia's firehose of falsehood is able to flood the information space of the majority of "connected" states around the globe, fomenting political divisions and creating crises and other opportunities for Russia to exploit. Without the development of countermeasures, the West may soon find itself falling prey to Russia's information warfare-enabled reflexive control strategies. Countermeasures must be both information-technical, such as enhanced detection methods for social media bot accounts, and information-psychological, such as enhanced education through the promotion of critical thinking in addition to digital and media literacy programs.

References

Arquilla, J and Karasik, T (1999) 'Chechnya: a glimpse of future conflict?', *Studies in Conflict and Terrorism*, 22(3), pp. 207–229. doi:10.1080/105761099265739.

Bartles, CK (2016) 'Getting gerasimov right', *Military Review*. US Army CGSC, 96(1), pp. 30–38.

BBC News (2005) 'Putin deplores collapse of USSR', *BBC News*. http://news.bbc.co.uk/2/hi/4480745.stm, accessed May 6, 2020.

Blank, S (2013) 'Russian information warfare as domestic counterinsurgency', *American Foreign Policy Interests*. Routledge, 35(1), pp. 31–44. doi:10.1080/10803920.2013.757946.

Cavegn, D (2017) 'Ansip, laaneots: Russian agents present during Bronze night riots', *Eesti Rahvusringhääling*. https://news.err.ee/592127/ansip-laaneots-russian-agents-present-during-bronze-night-riots, accessed May 6, 2020.

Chalupa, A (2014) 'Putin's fabricated claim of a fascist threat in Ukraine', *Forbes*. https://www.forbes.com/sites/realspin/2014/04/04/putins-fabricated-claim-of-a-fascist-threat-in-ukraine, accessed May 6, 2020.

Chertoff, M and Rasmussen, AF (2019) 'The unhackable election: what it takes to defend democracy', *Foreign Affairs*, 98, pp. 156–164.

Chotikul, D (1986) *The Soviet theory of reflexive control*. Monterey, CA: Naval Postgraduate School.

Cordesman, AH (2014) *Russia and the "Color Revolution"*. Center for Strategic & International Studies. https://www.csis.org/analysis/russia-and-color-revolution, accessed May 6, 2020.

Danchev, D (2008) '300 Lithuanian sites hacked by Russian hackers', *ZDNet*. http://www.zdnet.com/article/300-lithuanian-sites-hacked-by-russian-hackers/, accessed May 6, 2020.

Davis, J (2007) 'Hackers take down the most wired country in Europe', *WIRED*. https://www.wired.com/2007/08/ff-estonia/, accessed May 6, 2020.

Defense Science Board (2008) *Report of the defense science board task force on strategic communication*. Washington, DC. https://apps.dtic.mil/docs/citations/ADA476331, accessed May 6, 2020.

Dixon, R (1999) 'Chechens use net in publicity war with Russia', *Los Angeles Times*. https://www.latimes.com/archives/la-xpm-1999-oct-08-mn-20034-story.html, accessed May 6, 2020.

Duncan, PJS (2013) 'Russia, the West and the 2007–2008 electoral cycle: did the Kremlin really fear a "Coloured Revolution"?', *Europe–Asia Studies*, 65(1), pp. 1–25. doi:10.1080/09668136.2012.698049.

EU East Stratcom Task Force (2017) 'RT goes undercover as in the now', *EUvsDisinfo*. https://euvsdisinfo.eu/rt-goes-undercover-as-in-the-now/, accessed May 6, 2020.

Fawn, R and Nalbandov, R (2012) 'The difficulties of knowing the start of war in the information age: Russia, Georgia and the War over South Ossetia', *European Security*, 21(1), pp. 57–89. doi: 10.1080/09662839.2012.656601

Fayutkin, D (2006) 'Russian-Chechen information warfare 1994–2006', *RUSI Journal*, 151(5), pp. 52–55. doi:10.1080/03071840608522874.

Galeotti, M (2018) 'The mythical "Gerasimov Doctrine" and the language of threat', *Critical Studies on Security*, 7(2), pp. 1–5. doi:10.1080/21624887.2018.1441623.

GCHQ National Cyber Security Centre (2018) *Reckless Campaign of cyber attacks by Russian military intelligence service exposed*. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed, accessed May 6, 2020.

Gerasimov, V (2016) 'The value of science is in the foresight: new challenges demand rethinking the forms and methods of carrying out combat operations', *U.S. Army Military Review*. Translated by R Coalson, 96(1), p. 23.

Giles, K (2016) *Handbook of Russian information warfare*. Rome: NATO Defense College Research Division. http://www.ndc.nato.int/news/news.php?icode=995, accessed May 6, 2020.

Giles, K (2019) *Moscow rules: what drives russia to confront the west*. Washington, D.C.: Brookings Institution Press, pp. 35–58.

Giles, K and Hagestad, W (2013) 'Divided by a common language: cyber definitions in Chinese, Russian and English', *2013 5th international conference on cyber conflict*, Tallinn.

Greenberg, A (2017) 'The NSA confirms it: Russia hacked French election "Infrastructure"', *WIRED*. https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/, accessed May 6, 2020.

Haddick, R (2011) 'This week at war: Lessons from Cyberwar I', *Foreign Policy*. https://foreignpolicy.com/2011/01/28/this-week-at-war-lessons-from-cyberwar-i/, accessed May 6, 2020.

Hollis, D (2011) 'Cyberwar case study: Georgia 2008', *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008, accessed May 6, 2020.

Jonsson, O and Seely, R (2015) 'Russian full-spectrum conflict: an appraisal after Ukraine', *Journal of Slavic Military Studies*, 28(1), pp. 1–22. doi:10.1080/13518046.2015.998118.

Kishkovsky, S (2008) 'Georgia is warned by Russia against plans to join NATO', *The New York Times*. https://www.nytimes.com/2008/06/07/world/europe/07russia.html, accessed May 6, 2020.

Kramer, AE and Higgins, A (2017) 'In Ukraine, a malware expert who could blow the whistle on Russian hacking', *The New York Times*. https://www.nytimes.com/2017/08/16/world/europe/russia-ukraine-malware-hacking-witness.html, accessed May 6, 2020.

Lucas, E and Nimmo, B (2015) *Information warfare: what is it and how to win it?* Washington, DC: CEPA. http://infowar.cepa.org/Reports/How-has-Russia-Weaponized-Information, accessed May 6, 2020.

Ministry of Defense of the Russian Federation (2011) *Conceptual views regarding the activities of the armed forces of the Russian federation in the information space*. Moscow: Ministry of Defense. https://ccdcoe.org/uploads/2018/10/Russian_Federation_unofficial_translation.pdf, accessed May 6, 2020.

NATO Standardization Office (2019) 'Record 39182: cyberspace', *NATOTerm*. https://nso.nato.int/natoterm/Term.mvc/Display?termGroupId=39186, accessed May 6, 2020.

Office of the Director of National Intelligence (2017) *Assessing Russian activities and intentions in recent US elections, intelligence community assessment*. Washington, DC: Office of the Director of National Intelligence. https://www.dni.gov/files/documents/ICA_2017_01.pdf, accessed May 6, 2020.

Office of the President of the Russian Federation (2019) *National strategy for the development of artificial intelligence over the period extending up to the year 2030*. Edited by Konaev, M., Vreeman, A., and Murphy, B. Translated by Etcetera Language Group. Washington, DC: Center for Security and Emerging Technology, p. 490. https://cset.georgetown.edu/wp-content/uploads/Decree-of-the-President-of-the-Russian-Federation-on-the-Development-of-Artificial-Intelligence-in-the-Russian-Federation-.pdf, accessed May 6, 2020.

Oliker, O et al. (2015) *Russian foreign policy in historical and current context: a reassessment*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/perspectives/PE144.html, accessed May 6, 2020.

Pain, E (2000) 'The second Chechen War: the information component', *Military Review*. Fort Leavenworth: Department of the Army Headquarters, 80(4), pp. 59–69.

Paul, C and Matthews, M (2016) *The Russian "Firehose of Falsehood" propaganda model: why it might work and options to counter it*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/perspectives/PE198.html, accessed May 6, 2020.

RT (2017) '"Whoever Leads in AI Will Rule the World": Putin to Russian children on knowledge day', *RT*. https://www.rt.com/news/401731-ai-rule-world-putin/, accessed May 6, 2020.

Russian Federation (2000) *2000 information security doctrine of the Russian Federation*. Moscow: Russian Federation.

Russian Federation (2014) *The military doctrine of the Russian Federation*. Moscow. https://rusemb.org.uk/press/2029, accessed May 6, 2020.

Saeed, S (2017) 'US intelligence chief: Russia interfering in French, German elections', *Politico*. http://www.politico.eu/article/us-intelligence-chief-russia-interfering-in-french-german-elections/, accessed May 6, 2020.

Seddon, M (2014) 'Documents show how Russia's troll army hit America', *BuzzFeed News*. https://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america, accessed May 6, 2020.

Seely, R (2017) 'Defining contemporary Russian warfare', *The RUSI Journal*. Routledge, 162(1), pp. 50–59. doi:10.1080/03071847.2017.1301634.

Shea, TC (2002) 'Post-Soviet Maskirovka, cold war Nostalgia, and peacetime engagement', *Military Review*, 82(3), pp. 63–67.

Sieca-Kozlowski, E (2009) 'From controlling military information to controlling society: the political interests involved in the transformation of the military media under Putin', *Small Wars & Insurgencies*, 20(2), pp. 300–318. doi:10.1080/09592310902975430.

Sindelar, D (2014) 'The Kremlin's troll army', *Atlantic*. https://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/, accessed May 6, 2020.

Socor, V (2008) 'The goals behind Moscow's proxy offensive in South Ossetia', *Eurasia Daily Monitor*. Jamestown Foundation, 5(152). https://jamestown.org/program/the-goals-behind-moscows-proxy-offensive-in-south-ossetia/, accessed May 6, 2020.

Stent, AE (2014) *The Limits of Partnership*. New Jersey: Princeton University Press, pp. 97–123. doi:10.2307/j.ctv7h0twn.11.

Thomas, T (2016) 'The evolution of Russian military thought: integrating hybrid, new-generation, and new-type thinking', *Journal of Slavic Military Studies*. Routledge, 29(4), pp. 554–575. doi:10.1080/13518046.2016.1232541.

Thomas, TL (2003) 'Information warfare in the second (1999-Present) Chechen War: motivator for military reform?', in Aldis, A and McDermott, RN (eds) *Russian Military Reform 1992–2002*. London: Frank Cass, pp. 209–233.

U.S. Department of Homeland Security (2016) *Joint statement from the department of homeland security and office of the director of national intelligence on election security*. Washington, DC: Department of Homeland Security. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national, accessed May 6, 2020.

U.S. Joint Chiefs of Staff (2018) *JP 3–12 cyberspace operations*. Washington, DC: Department of Defense.

Whitmore, B (2008) 'Scene at Russia-Georgia border hinted at scripted affair', *Radio Free Europe/Radio Liberty*. https://www.rferl.org/a/Russia_Georgian_Scripted_Affair/1193319.html, accessed May 6, 2020.