Limits of Control: Examining the Employment of Proxies by the Russian Federation in Political Warfare

Matthew A. Lauder
Defence Research and Development Canada (DRDC)

Since the late 1990s, the Russian Federation has implemented several iterations of a security and defence sector revitalization program to meet emergent threats and challenges. In addition to the acquisition of new equipment and weapons systems, the revitalization program includes the development of a new operating construct, often referred to by Western military analysts and journalists as non-linear warfare or political warfare (as well as next generation warfare, remote warfare, hybrid warfare, and the Gerasimov doctrine), which guides the employment of military and non-military means by the Russian government to achieve geopolitical objectives (Lauder, 2018a). A central feature of Russia's political warfare construct is the utilization of proxies, most notably non-state actors. In fact, proxies – sometimes referred to as surrogates or surrogate forces (Krieg & Rickli, 2018) – are considered to be the primary protagonists of political warfare and conduct much of the 'heavy-lifting,' with the state services (i.e., the military and security agencies) playing a coordination and support role. It should also be noted that proxies are not limited to private military corporations and security companies, but include commercial enterprises (e.g., financial institutions, media conglomerates, public relations firms, and oil and gas companies, etc.), government-organized non-governmental organizations (GONGOS) and non-government organizations (NGOs), as well as professional associations and trade unions, think-tanks and academic centres, religious organizations, political groups, oligarchs, criminal organizations, patriotic groups, and paramilitary organizations and other state-sponsored militias (McGeady, 2017; Kozey, 2017). The political warfare construct also broadly empowers and leverages civilian and other non-combatant (sometimes referred to as compatriots) participation in political warfare, in particular for the planning and execution of information and psychological actions, such as protests and demonstrations as well as social media campaigns and computer network attacks. In other words, the Russian government has implemented a whole-of-society approach to political warfare in which proxies play an increasingly critical role (Troeder, 2019).

The purpose of this article is twofold. First, it examines the evolving nature and role of proxies employed by the Russian government in the execution of political warfare. Second, it proposes a conceptual model of the employment of proxies by the Russian government and briefly discusses the implication to the North Atlantic Treaty Organization (NATO). To accomplish this task, this article is divided into three sections. The first section discusses the characterization of

contemporary interstate conflict. This will be achieved by drawing upon and examining Russian strategic doctrine and policy. The second section discusses several recent examples of the employment of proxies by the Russian government in the execution of political warfare, namely Estonia (2007), Georgia (2008), Ukraine (Crimea and Donbas) (2014) and Syria (2013-2018). The third section briefly outlines three key trends in the employment of proxies and proposes a conceptual model of proxy employment by the Russian government and discusses the implication to NATO.

Section 1: Russian Political Warfare in Theory and Doctrine

Whereas NATO focused on the development of capabilities to conduct counter-terrorism (CT) and counter-insurgency (COIN) operations in the intermediate post-Cold War era, the Russian Federation, as part of a sweeping and aggressive security and defence sector revitalization program, continued to invest in and modernized its political warfare capability, which included new organizational structures, policies, doctrine and tactics (Trevithick, 2017; Chivvis, 2017). Moreover, the Russian government quickly embraced and integrated new and emerging technology into its political warfare capability (e.g., electronic warfare, cyber, social media and mobile technology) and utilized a range of proxies as a force multiplier (Iasiello, 2017; Spearin, 2018; Graja, 2019).[1] As a result, the Russian government achieved an asymmetric advantage over NATO, specifically in the conceptual space between peace and war (Trevithick, 2017). The following section provides an overview of strategic doctrine and policy guiding the employment of proxies by the Russian government.

Military Doctrine of the Russian Federation (2014)

Largely an update to the 2000 version, the 2014 edition of the military doctrine serves to revise and integrate concepts from several strategic documents (e.g., National Security Strategy, Foreign Policy Concept, etc.) (Ermus and Salum, 2017) and discusses a wide range of threats and risks to the Russian Federation (Trenin, 2014; Sinovets & Renz, 2015; European Parliament, 2017; Ruiz, 2017). For example, the doctrine notes that while large-scale war is now less likely, military risks and threats have shifted to the information space and the "internal sphere" (i.e., the Russian domestic context) (Government of Russia, 2015a). The doctrine explicitly identifies NATO enlargement and encroachment, as well as attempts by unnamed foreign entities to overthrow and destabilize legitimate and allied governments and states (in particular through the use of information and communication technologies), as a significant and evolving threat to Russian sovereignty and territorial integrity (Covoli, 2014; Sherr, 2017; Sinovets & Renz, 2015; Bender, 2015, European Parliament, 2017; Ruiz, 2017; Pynnoniemi, 2018). While the foreign

[1] Whether partisans, guerillas or front organizations, Spearin (2018) argues that Russia has significant experience in the employment or proxies. In other words, the Russian government, drawing up its Cold War experience, has "revisited" and modernized the employment of proxies for contemporary operating environment.

entities and allied governments were not explicitly identified in the doctrine, many analysts note the articulation was a clear reference to the Euromaidan demonstrations in Ukraine and perceived Western interference (Trenin, 2014; Pynnoniemi, 2018; Ruiz, 2017).

The doctrine also discusses the nature of contemporary conflict, which is characterized by the "integrated" employment of military and non-military measures, as well as the use of special forces, foreign-funded political groups and NGOs, irregular forces and private military corporations to amplify and support the "protest potential of the population (Government of Russia, 2015a)." The doctrine also argues that traditional military means have largely been replaced by indirect and asymmetric approaches and the application of simultaneous pressure across all environmental domains and throughout the depth of a targeted country (Sherr, 2017; European Parliament, 2017).

Russian Federation's National Security Strategy (2015)

Approved by Putin on 31 December 2015, and building upon the 2011 military doctrine, the National Security Strategy recognizes increased tension and the potential for conflict between the West and the Russian Federation (Government of Russia, 2015b; Oliker, 2016). For example, the strategy asserts that the West is intentionally "creating seats of tension in the Eurasian region" which is "exerting negative influence on Russia" and limiting Russia's ability to achieve geopolitical goals (Government of Russia, 2015b). Moreover, the strategy explicitly blames the continuing conflict in Ukraine on the West, specifically the US and European Union (previous documents only hinted or insinuated Western involvement). The strategy also warns the "overthrowing of legitimate political regimes and provoking intrastate instability" is increasingly widespread (Government of Russia, 2015b).

Similar to the military doctrine, the National Security Strategy identifies a number of threats to the Russian Federation (European Parliament, 2017; Pynnoniemi, 2018). According to the strategy, the main threats include extremist groups attempting to destabilize the government and disrupt society. The strategy also identifies "radical public associations" and foreign funded or sponsored NGOs as a threat to the Russian Federation, namely because they are recognized as undermining social and religious unity and serve as the primary catalysts of colour revolutions (Government of Russia, 2015b; McDermott, 2016).

Foreign Policy Concept of the Russian Federation (2016)

The *Foreign Policy Concept of the Russian Federation* was approved by Putin on 30 November 2016 and reflects the issues and threats identified in the *National Security Strategy*, noting that numerous (albeit unspecified) countries are using a range of military and soft-power (i.e., non-military) capabilities to achieve foreign policy objectives (Government of Russia, 2016a).

The concept also identifies and discusses a number of objectives for the Russian government, which many analysts believe to be a direct response to the use of soft-power by state competitors (i.e., the West), including strengthening Russia's geopolitical influence, promoting the Russian language and cultural identity of the Russian people, and defending the rights of the Russian speaking diaspora (e.g., promoting the concepts of Russkiy Mir and Russian compatriots) (Dyner, 2017; Sherr, 2017). As noted by Igor Zevelev (2016), between 2012 and 2016, the Russian government effectively blended concepts from the areas of national identity and culture, defence and security and foreign policy and international relations, resulting in the "seemingly irrational amalgamation of national identify narratives, international security discourse, and domestic security goals." The concept also explicitly states the Russian government will enhance and promote the standing of Russian mass media and communications tools "in the global information space" in order to "convey Russia's perspective (Government of Russia, 2016a)." Moreover, and building upon earlier iterations, the foreign policy concept expresses concern about a lack of objective international coverage about Russia and Russian actions abroad (Government of Russia, 2016a).

In response to these threats, the doctrine explicitly identifies the role of the Russian government as facilitating the development of an information security systems to counter foreign information and psychological actions, specifically attempts to undermine the "historical foundations and patriotic traditions" of Russia (Government of Russia, 2016b). These defensive activities include, but are not limited to, neutralizing attempts by various entities (state and non-state actors) to "erode Russian traditional moral and spiritual values" and providing Russians and the international community with "reliable information on the state and its position on socially significant events (Government of Russia, 2016b)." The doctrine also identifies the requirement of the Russian government to control and reinforce traditional spiritual and moral values, including the provision of youth-focused patriotic education programs (Darczewska, 2016; Ruiz, 2017).

Although a comprehensive examination of Russian military theorists and strategic doctrine is beyond the remit of this article, two common themes can be identified by the brief description above. The first theme is that non-military means are expected to play an increasingly important role in contemporary interstate conflict, to the point that it replaces the application of armed force and violence as the primary line of operation. The second theme is that proxies become the protagonists of contemporary interstate conflict, with state assets serving a coordination and support role.

Section 2: Examples of Proxy Employment in Contemporary Interstate Conflict

A central feature of Russia's political warfare construct is the utilization of proxies. This conceptualization of proxies is formalized and institutionalized in the broad set of Russian government strategic doctrines and policy. In fact, strategic doctrine and policy clearly identifies the need for the full and active participation of all actors from across the private and public sectors in political warfare. As such, proxies are not limited to private military corporations and security companies, but include the breadth of commercial enterprises, government-organized non-governmental organizations and non-government organizations, as well as professional associations and trade unions, think-tanks and academic centres, religious organizations, political groups, oligarchs, criminal organizations, patriotic groups, and paramilitary organizations and state-sponsored militias. Russia's political warfare construct also seeks to empower and exploit civilian and other forms of non-combatant participation in contemporary interstate conflict, further blurring traditional conceptual boundaries. The following section examines several recent examples of Russian government employment of proxies in political warfare, namely in Estonia (2007), Georgia (2008), Ukraine (Crimea and Donbas) (2014) and Syria (2013-2018).

Estonia (2007)

After a number of years of escalating tensions between Estonian nationalists and ethnic Russians over the proposed relocation of the Bronze Soldier statue, a Soviet World War II memorial located in a park in Tallinn, the Estonian government finally decided it would relocate the statue, along with a number of Soviet war graves, to a nearby war cemetery. To prepare for the exhumation of the graves, government workers set-up barriers and assembled a large tent over the site on 26 April 2007. Concerned that the statue was about to be moved, three members of Nochnoy Dozor (Night Watch), a volunteer group made up of ethnic Russians, attempted to block access to the site by refusing to move their vehicle. In response, police smashed the windows and forcibly removed the individuals from the vehicle.

Within hours of the confrontation between the police and the members of *Nochnoy Dozor*, more than a thousand protestors arrived at the site, most of whom were ethnic Russian. Although a small number of agitators attempted to climb over the barriers, the protest largely remained peaceful. Russian news media, however, started to report on the situation, and suggested it could quickly escalate into an ethnic conflict. In response, representatives of the Russian government, including Putin, referred to the removal of the statue as "an act of blasphemy," amounting to the "glorification of Nazism (Meyers, 2007)."

At dusk, however, the protest abruptly turned violent, as several hundred protestors, seemingly under the direction of several men, attacked the police (Cavegn, 2017).[2] As the violence started to increase and the scene descended into chaos, roaming bands of ethnic Russian protestors smashed windows and looted nearby stores. The rioting lasted much of the night, with police finally gaining control of the situation around 0300hrs. In the morning, more than 300 ethnic Russian protestors had been arrested. Dozens of police and protesters were also injured, and one protestor was stabbed to death (by an unknown assailant) (Meyers, 2007).

While much of 27 April was quiet, with hundreds of young ethnic Russian students protesting in front of government buildings, rioting broke-out in the late hours of the evening in several towns. By the morning of 28 April, several hundred more protestors were arrested, and nearly 200 people were injured, along with two dozen police officers.

April 28 through 30 were largely characterized by non-violent and peaceful protests by ethnic Russian activists, including a slow-moving motorcade through streets of Tallinn which caused significant traffic congestion. However, in Moscow, the Estonian embassy was effectively shut-down by Nashi members, a patriotic youth group, who prevented staff from exiting the building. The Estonian ambassador was also physically assaulted by Nashi members. In addition, a previously unknown militia group, identifying itself as the Army of Russian Resistance – Kolyvan (which is Russian for Estonia), posted a call to action along with political demands on several Russian language forums and chat rooms (Army of Russian Resistance, 2007). If their demands were not met, the group promised an armed revolt by 09 May, which was to include attacks on communications and transportation system, as well as electrical generation facilities and oil and gas infrastructure.[3] The group also called upon Putin to intervene and the Russian military to invade Estonia. However, beyond releasing calls to action and the threatening the Estonian government, the militia group never conducted any armed operations.

The rioting and protests were not limited to the physical environment; rather, a significant and seemingly synchronized cyber campaign was also executed by Russian activists (Traynor, 2007; Blank, 2008). The cyber campaign was conducted in two phases. The first phase started in the evening of April 27 and lasted until 03 May and included the recruitment and employment of Russian cyber activists, facilitated by a professional Russian hacker group, to conduct human-in-the-loop DoS attacks (i.e., ping attacks) and website defacements (Davis, 2007). Using Russian language chat rooms and forums, the hacker group provided the tools and targets for Russian cyber activists to engage in a coordinated, albeit a rudimentary, cyber campaign, largely targeting political parties and institutions (Ruus, 2008). Essentially using the massing of

[2] Estonian authorities believed the protests were coordinated by Russian agents, including operatives from the GRU.

[3] 09 May is an important date in the Russian calendar, as it marks the national day to commemorate the Soviet victory over Nazi Germany in WWII.

individually conducted DoS attacks as cover (i.e., what appeared to be a cyber riot), the hacker group targeted and defaced political websites (posting a fake apology letter from the Estonian Prime Minister) and used bots to effectively saturate Estonian news media discussion forums with negative comments about the Estonian government (Davis, 2007). A forensic analysis of the attacks by cyber experts indicated that some of the IP addresses involved in the initial attacks directed back to Russian addresses, including the Russian government (Traynor, 2007).

The second phase of the cyber campaign ran from 04 to 18 May, when the attacks abruptly ended. Unlike the first phase, the second phase was largely conducted by professional hackers and involved relatively sophisticated techniques and a high-degree of operational knowledge about the Estonian network and potential counter-measures. The second campaign also required significant financial backing. For example, the Russian hacker group set-up anonymous Pay Pal accounts and rented a large number of botnets for specific periods of time (the botnets were generally used for commercial email spamming) (Ruus, 2008). In essence, this approach allowed the Russian hacker group to conduct numerous and simultaneous multi-target brute-force DDoS attacks by sending high volumes of email traffic to specific servers from different locations around the world, which resulted in widespread outages across Estonian governmental, communications and financial sectors, in particular online banking (more than 90% of Estonians used Internet-based banking and ATMs) (Traynor, 2007; Ruus, 2008). Moreover, the hacker group successfully evaded defensive filtering and DNS (Domain Name System) sinkholes by constantly changing tactics and targets, as well as a modifying the software.

By the end of the physical and cyber riots, more than 1300 Russian protestors had been arrested, and dozens of protestors and police officers were injured. In addition, hundreds of stores, houses and vehicles were damaged, and Estonian government and financial sectors, as well as news media outlets, experienced prolonged outages and the vast majority of Estonians were impacted due to a lack of access to communications systems and online banking (Davis, 2007). Although Konstantin Koloskokov, the Transnistrian Nashi commissar, claimed responsibility for the cyber campaign against Estonian infrastructure, many experts believe Koloskokov and the youth group was used as cover by the Russian government in order to evade responsibility (Shachtman, 2009; Keating, 2010).

Georgia (2008)

It is difficult to identify the exact incident that triggered the five-day war between Georgia and Russia in August of 2008 (Chivers, 2008; Finn, 2008; Clover, Belton, Dombey & Cienski, 2008; Chausovsky, 2018; Chivers & Barry, 2008). At the time, many analysts blamed Mikheil Saakashvili, the Georgian President, for being impulsive and reckless, suggesting he was the antagonist and that Russia was merely coming to the defence of South Ossetia (van Herpen,

2015); which is how the Russian government wanted the conflict to be portrayed by the international news media (Iasiello, 2017). However, that assertion has been revisited in a number of journalistic and scholarly accounts of the war (Koffman, 2018a). In actuality, the military operation had been carefully planned and executed by the Russian government, supported by a "process of gradual and purposive escalation" since 2000 and culminating in a series of hostile actions conducted by the Russian government and its proxies in the weeks preceding the incursion of Georgian military forces into South Ossetia on 07 August 2008 (van Herpen, 2015; Pallin & Westerland, 2009). These hostile actions included, but were not limited to, an assassination attempt on Dmitry Sanakoev (the head of the Georgian-backed administration in South Ossetia), repairs to railroads by Russian railroad troops in Abkhazia (to facilitate the movement of troops and military equipment into the area), attacks on Georgian police officers and the shelling of several Georgian towns by South Ossetian militias, public declarations that upwards of 2000 Cossack militias and other military volunteers were deploying to help defend the region (Staff Writer, 2008; Bondarenko & Sas, 2008), and a series of computer network attacks that effectively shut-down or limited the ability of the Georgian government to communicate with the public (Connell & Vogler, 2017).[4] [5] [6] In essence, the Russian government carefully manufactured the crisis and effectively goaded the Georgian government into initiating hostilities, which became a "convenient pretext to launch a full-scale, multi domain invasion (Beehner et al., 2018)." In a ten-year anniversary retrospective on the conflict, Michael Kofman (2018a) notes that Saakashvili "stepped into a trap designed by Putin to take advantage of the Georgian leader's ambitions, fears and inexperience."

After a week of increasingly violent skirmishes between South Ossetian militias and Georgian security forces that included exchanges of artillery fire into residential areas and based upon communications intercepts indicating Russian troops were preparing to enter South Ossetia through the Roki Tunnel, Saakashvili gave the order for the Georgian military forces to mobilize and advance towards South Ossetia on the early afternoon of 07 August 2008 (Barabanov, Lavrov, Pukhov & Tseluiko, 2010). At around the same time, Georgian personnel left the Joint

[4] Cyber analysts noted a series of distributed denial of service (DDoS) attacks originating from Russia and directed towards Georgia's internet infrastructure as early as 20 July 2008. The DDoS attacks involved a stream of data packets that contained the message, "win+love+in+Rusia," which was designed to overload Georgian government internet servers (Markhoff, 2008). As a result, the Georgian President's website was taken offline for nearly a day.
[5] Seemingly expecting the outbreak of war, the Russian government organized a visit to South Ossetia by more than 50 journalists representing most of the leading Russian news media outlets, including but not limited to ITAR-TASS, REN TV, Ria Novosti, and MIR. Russian authorities also transported thousands of South Ossetians to Russia, effectively emptying Tskinvali of non-combatants prior to the conflict. Both activities suggest that the Russian government not only expected but planned the outbreak of hostilities (van Herpen, 2015).
[6] Although extending over several years prior to the outbreak of war, the Russian government engaged in a campaign of 'passportification;' that is, providing Russian citizenship and passports to residents of South Ossetia and Abkhazia. The purpose of campaign was to provide justification for military intervention based on the notion of their right to protect Russian citizens (van Herpen, 2015).

Peacekeeping Force (JPKF) headquarters, which included Russian, Georgian and South Ossetian personnel, in Tskhinvali.[7] Although the situation was quickly spiralling out of control, Saakashvili hoped that, by pushing his forces towards South Ossetia, he could put an end to the artillery strikes and prevent Russian forces from entering the region through the Roki Tunnel.

Saakashvili ordered a unilateral ceasefire at approximately 1900hrs on 07 August 2008. The decision was largely based upon a meeting between Georgian and Russian representatives in Tskhinvali at which the Russian commander of the JPKF admitted he had no control over the South Ossetian militias. In addition, and due to a lack of control, the Russian commander advised Georgian authorities to implement an order to unilaterally halt hostilities. In a live television address, Saakashvili updated the Georgian public on the situation and called for negotiations with Russian and South Ossetian leadership. He also reaffirmed the promise of unrestricted autonomy for South Ossetia and pleaded for international assistance to help stop the violence. However, Russian military commanders regarded the ceasefire as a deception designed to buy time and allow Georgian commanders to deploy additional troops for offensive operations against South Ossetian positions. Ironically, South Ossetian militias exploited the ceasefire and escalated their attacks, using the unilateral declaration as an opportunity to shell several Georgian towns, which forced hundreds of civilians to flee the area. By late evening on 07 August, it was clear that South Ossetian militias had no interest in the participating in negotiations. In response, Saakashvili, at 2335hrs, gave the order for Georgian defence forces to push into South Ossetia.

Early in the morning on 08 August 2008 (sometime between 0200 and 0530hrs), two Russian motorized rifle brigades started to pass through the Roki tunnel and enter South Ossetia.[8] The brigades, which were a part of the Russian 58th Army and based at Vladikavkaz in North Ossetia, recently participated in Kavkaz-2008 (Caucasus-2008), a joint counter-terrorism and peacekeeping exercise, and were essentially waiting for the order to mobilize since 02 August. However, by the time Russian forces started to move en masse, Georgian defence forces made significant gains, effectively taking control of Tskhinvali, as well as other strong points, by 0830hrs. Vladimir Putin, then Russian Prime Minister, denounced what he referred to as Georgian aggression against South Ossetia, and threatened a Russian response. Russian journalists, many of whom were prepositioned by the Russian government in Tskhinvali days

[7] The Russian peacekeeping force was made up of border troops, but also Spetsnaz forces. In Abkhazia, the Russian peacekeeping unit was reinforced by artillery and other stand-off weapons (van Herpen, 2015; Kofman, 2018a; Pallin & Westerlund, 2009).

[8] There is evidence to suggest that small elements of the 58th Army were deployed and arrived in South Ossetia by 07 August 2008, a day prior to the official start of hostilities (van Herpen, 2015).

prior to conflict, started to accuse Georgian authorities of conducting atrocities against civilians in South Ossetia (van Herpen, 2015).[9] [10]

By late-afternoon on 08 August, and after a number of small skirmishes and air assaults on Georgian military positions, the Russian 58th Army closed in on Tskhinvali; the stage was set for major combat operations. Additional Russian troops had also arrived in South Ossetia, or were on their way, including Airborne and Spetsnaz forces, as well as naval and air assets (Barnard, 2008).[11] Over the course of the evening and into the morning of 09 August, violence increased dramatically, and both sides reported casualties, including that of Lieutenant General Anatoly Khrulyov, the commander of the Russian military forces in South Ossetia, who was wounded by a Georgian reconnaissance unit during an ambush near Tskhinvali (Kofman, 2018b). Computer network attacks targeting Georgian government and civilian infrastructure also peaked on 08 August, involving both distributed denial of service (DDoS) and defacements that temporarily shut-down the websites of the Georgian President, as well as the Ministry of Defence and Ministry of Foreign Affairs (Danchev, 2008). In addition, several Georgian state computer

[9] Claims of genocide, ethnic cleansing and other atrocities conducted by the Georgian military by Russian authorities, including public statements by Medvedev, Putin and Sergei Lavrov (the Russian Minister of Foreign Affairs), and echoed by the Russian news media, persisted throughout the conflict. These claims were later determined to be false by an independent inquiry. In fact, most of the war crimes conducted during the war were committed by South Ossetian militias, who followed advancing Russian troops and engaged in a haphazard campaign of vandalism, rape, murder and looting (van Herpen, 2015; Harding, 2008). Russian troops were also involved in looting, as well as using cluster munitions against civilian targets, including the market in the centre of Gori (Clover, Belton, Dombey & Cienski, 2008; Barabanov, Lavrov, Pukhov & Tseluiko, 2010).

[10] Accusations of genocide and other atrocities by the Russian news media lasted throughout the conflict, even when evidence was mounting that Russian troops and irregular forces were involved in war crimes, and was a key feature of the information campaign conducted by the Russian government, which was augmented by robust and prolonged cyber-attacks that sought to eliminate or limit the ability of the Georgian government to communicate with its own population, as well as international audiences.

[11] Spetsnaz forces deployed to South Ossetia included two units based in Chechnya, including a company-sized element of the Vostok battalion. Unlike other defence forces in Chechnya, the Spetsnaz forces did not report to and existed outside of the Chechen military leadership but were rather under the authority of the Russian Ministry of Defence (MOD), specifically the GRU. However, Vostok was more of a personal or family militia than a regular or formal military unit, as Yamadayev inherited command of the unit upon his brother's death in 2003, and his two younger brothers served as company commanders in the unit (McGeady, 2017). In Chechnya, members of the unit are referred to as *Yamadayevtsy*, and are known to be involved in a mix of warfare and criminal behaviour. The fact that the unit reported to Russian authorities created considerable tension with Ramzan Kadryov, the President of Chechnya, which eventually lead to a shoot-out on a highway between his personal security unit and members of the Vostok battalion (Staff Writer, 2008b). During the conflict with Georgia, Sulim Yamadayev, the commander of the Vostok battalion, was under an arrest warrant, which was later rescinded by authorities in Moscow (Barry & Schwirtz, 2009). Yamadayev was relieved of command of the Vostok battalion in late August 2008. On 29 March 2009, Yamadayev was assassinated in Dubai. Adam Delimkhanov, a member of the Russian State Duma for the United Russia party and cousin of Kadyrov, is believed to have ordered the assassination. Although numbers were never officially released, it is believed the Vostok battalion suffered numerous casualties in the Russian-Georgian war. It should be noted that, unlike other Russian military units and militias, the Vostok battalion was never implicated in any war crimes during the war.

servers came under external control, which seemed to be timed to the arrival of Russian troops in South Ossetia.

Putin, who was attending the 2008 Summer Olympics in Beijing, China, arrived in North Ossetia on the evening of 09 August. During a meeting with military leadership, which was later televised, Putin stated the actions of Georgia were tantamount to criminal behaviour, and that there would be no returning to the "status quo (Barnard, 2008)." Putin also stated that more than 30,000 refugees had sought shelter in Russia, and that dozens of civilians were killed (other Russian representatives stated that thousands of South Ossetian civilians were killed by Georgian forces). Putin also referred to the incursion of Georgian defence forces into South Ossetia as a "complete genocide (Dzhindzhikhashvili, 2008)." Apparently frustrated at the lack of progress of the Russian military, Putin took command of the military operation and ordered the Pskov-based 76th Airborne Division to assume control of the operation in South Ossetia (Kofman, 2018a; Beehner et al., 2018). In addition, Putin ordered a second front be opened up through Abkhazia (Barnard, 2009).

Over the next three days, and despite a willingness on part of Georgian authorities to negotiate an end to the hostilities, Russian troops and militias from South Ossetia and Abkhazia conducted numerous offensive operations and assaults against Georgian military positions, and Russian forces shelled and then advanced into the city of Gori, less than 90kms from Tbilisi and 27km from the Georgia-South Ossetian boundary. Russian troops also advanced into Zugdidi, near the boundary with Abkhazia, as well as the port city of Poti. Russian forces also conducted numerous airstrikes against Georgian civilian infrastructure, including the Tbilisi Airport. In defence of the continued aggression, Russian political and military representatives stated the Georgia request for peace negotiations was merely a stalling tactic to allow them to regroup and conduct a counter-offensive.

Hackers, believed to be affiliated with the Russian Business Network (RBN), a cyber-based organized crime group, continued to conduct coordinated computer network attacks, including redirecting significant portions of Georgia's internet traffic through servers in Russia (Swaine, 2008; Keizer, 2008; Danchev, 2008). Using the website, *stopgeorgia.ru*, and calling upon the support of patriotic hackers and internet users (i.e., to enlist the masses), Russian hackers (later determined to be affiliated with state security services) recruited people through Russian language social media sites and launched a website providing technical advice on how to set-up and execute DDoS and spam attacks (Turovsky, 2018; Rutherford, 2009; Leydon, 2009). The website also provided links to bespoke software to execute the attacks (e.g., ping floods and spamming) on Georgian infrastructure, as well as target list (of websites and emails) (Turovsky, 2018; Rutherford, 2009; Shakarian, 2011). The objective was to mobilize and leverage patriotic Russians to conduct, or at least support, a broad but decentralized cyber campaign against

Georgian communications infrastructure. In other words, Russian hackers, operating on behalf of the Russian government, created and utilized a legion of patriotic *script kiddies* to create a cyber militia and conduct computer network attacks (White, 2018 A40). This effort also turned cyber criminals, who typically conduct hacking operations for profit, into state-managed assets (Turovsky, 2018; Shakarian, 2011). Russian hackers also conducted a highly targeted defacement campaign, replacing images on the Georgian President's website with one that compared him to Hitler, along with text stating, "And it will end for him the same way." The *South Ossetia Hack Crew*, a previously unknown hacker group, took credit for the defacement (see Figure 1: Defacement of Georgian President's website) (Danchev, 2008). In total, more than 54 Georgian government, civilian and commercial websites, including law enforcement, news media websites, financial institutions and the constitutional courts, were temporarily taken offline or targets of defacement activities (Hollis, 2011; Iasiello, 2017; Shakarian, 2011; Swaine, 2008; Moses, 2008). As noted by Beehner et al (2018), a "patchwork of state, criminal and citizen-led actors" successfully undermined the Georgian ability to operate in the information environment, albeit for limited periods (White, 2018; Hollis, 2011).

Figure 1: Defacement of Georgian President's Website (Danchev, 2008).

By 13 August 2008, the conflict was largely but not entirely over, as Medvedev and Saakasvili agreed to a peace plan negotiated by France. US representatives, however, cautioned against the agreement, as its vague and ambiguous wording, in particular the caveat that allowed Russia to implement "additional security measures" as it deemed necessary, had the potential to allow the Russian government to "do almost anything (Meyers, 2008 A9)." Within hours of signing, and in violation of, the agreement, a Russian armoured column left Gori and headed for

Tbilisi. Exploiting the situation, South Ossetian militias and Russian irregular forces, including Cossacks, followed the advancing column and looted and burned several Georgian villages and executed several civilians (Harding & Meikle, 2008; Harding, 2008; Steele, 2009). The Russian armoured column finally stopped at Igoeti, about an hour west of Tbilisi, and dug reinforced defensive positions.

On 15 August, Condoleezza Rice, the US Secretary of State, meet with Saakashvili for about five hours, after which he officially signed the ceasefire agreement (Meikle & Traynor, 2008). Rice, at a news conference, publicly declared the requirement for Russian troops to immediately leave Georgian territory (Meyers, 2008). In response, Medvedev stated that Russian troops would start to withdraw by 18 August and that all Russian troops would be out of Georgia by 22 August (Torchia, 2008). A sizeable contingent of Russian troops, however, remained in Georgia (specifically in Gori, Zugdidi, and Poti) for at least another ten days, some of whom were involved in rampant looting and vandalism while other troops confiscated or destroyed Georgian military equipment, including coast guard vessels (Torchia, 2008; Meyers, 2008). On 26 August, Medvedev signed a Presidential decree recognizing the Republics of South Ossetia and Abkhazia as independent states. The decree also authorized cooperation and mutual assistance agreements with both countries.

Contrary to Russian claims of genocide and thousands of civilians being slaughtered by the Georgian military and security forces throughout the conflict (Barnard, 2008), the five-day conflict resulted in 67 Russian military personnel killed and 283 wounded, along with 365 South Ossetian militia personnel and civilians killed. A total of 170 Georgian military personnel, 14 police officers and 228 Georgian civilians were killed (Council of the European Union, 2009).

Ukraine: Crimea (2014)

The Russian military operation to annex Crimea started on 20 February and lasted until 22 March 2014 and involved significant and wide-ranging employment of proxies to set political conditions as well as to seize Ukrainian government and military facilities. Proxies were also critical to Russia consolidating territorial and political gains (Lauder, 2018a). In fact, while the Russian military did most of high-risk and tactically challenging tasks (albeit under the guise of being a local defence force), proxy forces played a critical support role, including – in some very specific cases – the planning and execution of armed raids (Lauder, 2016).

Between 20 and 25 February, several activities set the conditions for the deployment and arrival of the vanguard of the Russian military force and the seizure of the Crimean parliament buildings. For example, Russian military and security services prepositioned agents and other operatives in Crimea to mobilize local sympathizers, collect intelligence, organize demonstrations, recruit members for self-defence units, and disseminate Russian propaganda.

Members of the Night Wolves, a Russian patriotic biker club based in Moscow but with chapters throughout Europe and more than 5,000 members, were active throughout the operation collecting intelligence on behalf of the Russian military (Lauder, 2018b).[12] The Night Wolves also worked closely with a small unit of Russian Special Forces, which arrived in Crimea sometime between 22-23 February, to collect intelligence and help identify potential targets (Lauder, 2018b). During this period, Russian activists and members of Berkut, a paramilitary police force responsible for the murder of a number of Maidan protestors in Kiev, set-up barriers and conducted vehicle checkpoints, essentially cutting off Crimea from the rest of Ukraine (Traynor, 2014). On 25 February, several hundred Russian protestors rallied at the Crimean parliament buildings in Simferopol and demanded a referendum on separation from Ukraine and formally joining Russia.

On 26 February, Putin ordered a surprise inspection of combat readiness of the Western Military District. While the inspection was not unusual and most of the units followed prescribed deployment instructions, a small contingent of Spetsnaz and Airborne troops used the larger troop movement as cover to infiltrate Crimea (Norberg, 2014). In the early morning of 27 February, approximately 50 armed personnel in Russian uniforms but lacking any identifying rank or insignia (i.e., sterilized uniforms) seized the Crimean parliament building. While the armed personnel spoke Russian and identified themselves as being a local self-defence group, a leaked video of the raid clearly indicated they were a combined force of Russian Special Forces, Spetsnaz and Airborne troops (Lauder, 2018a). Later in the day, the armed group confiscated cell phones and oversaw a vote by the Crimean parliament to replace the pro-Kiev Crimean prime minister with a Russian politician.

Concerned about the numerical disadvantage (Ukraine had approximately 25,000 defence and security forces in Crimea), and taking advantage of preauthorized (by the Ukrainian government) resupply runs to leased military bases in Crimea, the Russian government used cargo and landing ships, as well as transport aircraft, to move additional troops and equipment into Crimea (Lauder, 2018a). By evening of 28 February, the Russian government successfully augmented its existing force structure in Crimea with several Mi-35 attack helicopters and several hundred Spetsnaz troops. During this period, the Night Wolves, as well as other recently organized self-defence groups, started to seize and occupy government and administrative buildings, as well as communications infrastructure. Russian operatives in Crimea and Russia also used SMS text and social media platforms to mobilize local activists and to recruit fighters in Russia (referred to as “tourists”) to serve in Crimean self-defence groups, effectively giving the military operation the appearance of a local uprising (Lauder, 2016).

[12] At least 11 members of the Night Wolves, including Alexander Zaldostanov, the president of the biker group, were awarded the campaign medal “For the Return of Crimea” from the Russian government (Lauder, 2018b).

The military operation in early March largely involved Russian Spetsnaz and Airborne troops (still in sterilized uniforms) negotiating with local Ukrainian military commanders and confiscating military bases and equipment, as well as government infrastructure. To bolster local self-defence units, several hundred Cossack militia members arrived in Crimea via the Kerch ferry from Russia, many of whom provided security at the Sochi Winter Olympics (Lauder, 2016; Lavrov, 2015).

Operating under the name Cyber Berkut, Russian hackers – and possibly a sub-unit of or a semi-independent group funded by the GRU – also conducted a significant cyber campaign against the Ukrainian government communications infrastructure (Lauder, 2019). Using DDoS attacks, defacements, cyber-squatting and redirects,[13] Russian hackers effectively eliminated the ability of Ukrainian politicians to communicate both internally and externally (Lauder, 2016). Looking to generate broad social and political effects, Russian hackers also targeted Ukrainian police and security services, NATO, as well as Ukrainian journalists (Lauder, 2018a).

Recognizing that most of the self-defence units lacked proper military training and discipline and concerned about significant casualties and collateral damage if employed in high-risk situations, Russian military commanders decided against using self-defence groups to support the forceful removal of Ukrainian soldiers from military installations in Crimea. As a result, self-defence units, including members of Berkut, were relegated to operating blockades and vehicle checkpoints, conducting unarmed patrols of the perimeter of Ukrainian military bases (but under the supervision of Russian soldiers), and providing security at Russian demonstrations (Lauder, 2018a). Self-defence groups also guarded Russian controlled administrative and government buildings. Although the Russian government made an effort to mitigate the risk, self-defence groups were still involved in several ignominious incidents, in particular the harassment and intimidation of Western journalists (Lauder, 2018a; Lauder, 2019).

There were, however, two exceptions. Both the Night Wolves and the Rubezh (which was comprised of recently retired members of the Russian marines and Spetsnaz) were permitted to conduct independent armed operations (Lauder, 2016; Lauder, 2018b). For example, the Night Wolves conducted a number of armed raids on communications and natural resources infrastructure, as well as capture operations of Ukrainian defence and security personnel. Likewise, the Rubezh conducted armed boarding parties of Ukrainian naval vessels.

Although there was a brief break from offensive military operations immediately prior to and following the Crimean sovereignty referendum on 16 March, Russian military commanders were eager to terminate the operation. Using non-lethal means, Spetsnaz and Special Forces

[13] The redirects automatically forwarded an internet user, without his or her knowledge, to a website that mimicked the Ukrainian government website but was under the control of Russian operatives.

units removed the remaining Ukrainian soldiers from several military bases in Crimea in just a few days.

By 22 March, the military operation to annex Crimea was over. In total, more than 20,000 Ukrainian military personnel defected, surrendered or were captured, and only one Ukrainian soldier, one Russian soldier, and three civilians were killed or died during the operation. Nearly a month later, Putin admitted to the presence of Russian troops in Crimea during a television interview. Referring to Crimea as "New Russia," Putin stated the military was in Crimea only to support local self-defence groups and help protect the Russian-speaking population, effectively maintaining the narrative that the annexation was a locally inspired and organized revolution (Makarechi, 2014; LoGiurato, 2014).

Ukraine: Donbas (2014)

Although the war in the Donbas region of Ukraine (consisting of Luhansk and Donetsk oblasts) between the Russian military and its proxies and the Ukrainian government continues to this day, for the purposes of this examination, the timeline of Russia's invasion and de facto annexation of Donbas can be identified as 20 February 2014, when Victor Yanukovych[14] fled to Russia, through the end of September 2014, with the signing of the first Minsk Protocol[15] and the establishment of a relatively stable line of demarcation between Ukrainian and Russian forces.

Immediately following Yanukovych's departure from Ukraine (first to Crimea, and then to Moscow), Russian hackers, operating under the moniker Cyber Berkut, escalated an ongoing DoS campaign targeting Ukrainian government websites, as well as the VOIP telephone network and cell phones of Ukrainian parliamentarians (Lauder, 2016). The campaign, which generally lacked technical sophistication, was still highly effective in that it limited the ability of Ukrainian parliamentarians and government employees to communicate with the public. By 27 February, however, nearly all communications between Kiev and Crimea were severed.

From late February through mid-April 2014, local Russian activists organized and conducted a series of demonstrations and protests, including seizing and occupying government buildings, across eastern Ukraine (Sakwa, 2016). However, these activities were not entirely spontaneous, nor were they locally inspired; rather, most were organized and funded by Yanukovych, with assistance from Russian intelligence services. In response, the Ukrainian state security services made an effort to regain control of the situation by removing protestors and arresting Russian intelligence operatives, most of who were from the GRU. Ukrainian state security services also

[14] Elected in 2010, Victor Yanukovych was the fourth president of Ukraine. He is currently living in exile in Russia.
[15] Signed by political representatives from Ukraine, Russian Federation, Donetsk Republic and Luhansk Republic on 05 September 2014, the Minsk Protocol was an agreement to halt armed conflict in the Donbas region of Ukraine.

arrested a number of Russian intelligence agents attempting organized local groups that would conduct acts of subversion and sabotage (Lauder, 2018a). Towards mid-April, Russian protestors became more brazen and started to raid police armouries and seize weapons, including assault rifles. During this period, Russian protesters in Donetsk also unilaterally declared the formation of the Donetsk People's Republic (DPR) and unification with Russia. By the middle of April, the political situation across Donbas was spiraling out of control.

Realizing an opportunity was emerging, Igor Girkin (Strelkov), and approximately 50 armed men (most of who were recently retired Russian military, including Spetsnaz), departed Crimea and arrived in eastern Ukraine on 12 April (Barabanov, 2015; Kuzio, 2017). Within a matter of days, Girkin was able to recruit approximately 200 local fighters and started to confront Ukrainian military and police forces. Shortly thereafter, other local Russian militias started to coordinate their activities with Girkin (although still operating as relatively independent groups).[16] By the end of April, Girkin assumed loose command (some units coordinated activities, but still operated as independent units) of all Russian militias operating under the banner of the Donbas People's Militia.

During late April, the FSB started to facilitate the movement of a significant number of Cossack fighters from Crimea into Donbas, as well as coordinating sabotage and political subversion activities by Russian activists and other operatives. Intelligence operations conducted by the Ukrainian state security services also suggest the GRU was responsible for coordinating much of the activity of Russian militias in eastern Ukraine, including the provision of weapons and other equipment, and that a Russian fringe political party was actively supporting militia activities (Lauder, 2018a; Sakwa, 2016).

By the end of April, Russian separatists were in control of a large portion of Luhansk. However, a lack of unified command and control (C2), plus dozens of relatively independent and ideologically divergent armed groups, severely limited the ability of Russian militias to

[16] Between March 2014 and the formal establishment of the United Armed Forces of Novorossiya (NAF) in September 2014, which combined the units serving under the command of the Donbass People's Militia and the Luhansk People's Militia as well as a number of autonomous or independent armed groups into – ostensibly – a unified fighting force, several dozen militias emerged and conducted military operations. Some of the early militias expanded and, upon joining the NAF, ultimately became battalion or brigade formations. Militias that did not swear allegiance to the republics of Donetsk and Luhansk were treated as criminal gangs and disarmed. In some cases, the leadership of 'troublesome' units were forcibly removed, sometimes through assassination. Militias groups operating in the summer of 2014 include, but are not limited to, the Vostok Battalion, OPLOT battalion, Prizrak (Ghost) Battalion, the Night Wolves, Rusich Company, Sparta Battalion, 1st Sloviansk Brigade, and Wolves' Hundred (Cossacks). Two points should be noted. First, some early militias assumed new monikers over the summer of 2014, especially when the unit grew in size and stature, while other units were disbanded due to high casualties. Second, militia members were not only from Ukraine and Russia, but also from across Europe. As such, several international battalions were formed, including Chechen, Greek, Ossetian, Polish, Serbian, Spanish and German.

consolidate control of the entire Donbas region. These factors also prevented Luhansk pro-Russian political leadership from making clear demands and negotiating a political settlement with authorities in Kiev (Lavrov, 2015).

Early May, however, represents the transition from relatively unstructured civil demonstrations by Russian activists and limited military engagements to a more coherent military campaign conducted by Russian militias (Lauder, 2018a). It also represented a discernible increase in the intensity of violence, by both Russian protestors as well as Russian militias. For example, on 02 May, after a day of clashes between Ukrainian and Russian protestors in Mariupol, several people were shot and injured and approximately 30 Russian protestors were killed when the building they were occupying was set ablaze. Dozens of Russian activists were also arrested. Days later, approximately 60 members of a Russian militia group seized the police headquarters in Mariupol, and successfully defended it against several counter-attacks by Ukrainian government forces. Russian militias then planned and executed a series of well-coordinated assaults and ambushes throughout the month of May, including numerous radio and television broadcast facilities, commercial airports and Ukrainian military bases and outposts. By the end of May 2014, Russian militias were on the offensive, having dealt Ukrainian government forces several embarrassing defeats.

Possibly buoyed by the success of the military campaign, Russian politicians in Luhansk and Donetsk announced the establishment of Novorossiya (New Russia) on 24 May, a day prior to Ukrainian general election. In addition, Cyber Berkut successfully hacked the servers of the Central Election Commission and surreptitiously installed malware on the election network that would show (contrary to the actual results) the Right Sector party leader as winning the vote by a narrow margin. However, the plan was thwarted just before the announcements of the election when a Ukrainian government cyber response team noticed and removed the malware (Lauder, 2018a).

June and July were characterised by fierce fighting with both sides experiencing significant personnel and equipment loses. However, by early July, it was clear that Ukrainian government forces were starting to make some small territorial gains, slowly pushing Russian militias further eastward. To prevent the collapse of the separatist movement and the loss of territorial gains, the Russian military started to secretly provide troops, weapons and other equipment (including vehicles) to the Russian militias, some of which was funneled to front lines by smuggling networks operated by criminal groups. Utilizing an extensive social and business network, the Night Wolves also played a central role in providing travel documents to and transporting several high-level Ukrainian government defectors to Russia as well as recruiting fighters to serve with Russian militias (Lauder, 2018b).

On 17 July, Malaysia Airlines Flight MH17, flying from Amsterdam to Kuala Lumpur, was shot down over Donetsk by a ground-to-air missile. The commercial plane, which was carrying 283 passengers and 15 crew members, was shot-down at approximately 33,000 feet. While both Ukrainian government forces and Russian militias immediately denied responsibility for the tragedy, the Russian government engaged in an extensive and multipronged disinformation campaign designed to blame the Ukrainian government (Lauder, 2018a). Within days, Russian state and aligned news media outlets, as well as social media trolls (from the Internet Research Agency, a social media company based in St. Petersburg, Russia) started a well-coordinated information campaign accusing the Ukrainian government of accidently shooting-down MH17 in a botched attempt to assassinate Putin.

By August 2014, and recognizing the Ukrainian government was making significant gains in eastern Ukrainian, the Russian government increased its support, including troops, equipment and weapons, to Russian militias. The Russian military also fired rocket and artillery systems across the border in support of Russian militia operations, which (on several occasions) forced Ukrainian troops to retreat. In other operations, Russian militias, backed by Russian troops, successfully surrounded and forced Ukrainian government forces to vacate some of their positions. However, other than a handful of small successes, such as the siege of Luhansk Airport in which a number of Russian militias, including the Night Wolves, eventually forced Ukrainian forces to abandon their positions, the Russian separatist movement was largely losing ground in the first half of August.[17]

In late August, approximately 250 Russian military vehicles, including armoured vehicles, tanks and artillery, followed by an additional two columns of tanks and more than 1000 soldiers entered Ukraine and conducted a three-pronged attack against Ukrainian forces defending Mariupol. Although the Russian government denied involvement or that its troops were operating inside Ukraine, some estimates suggest that (by the end of August) nearly 90% of the combat capability of the Russian militias was made up of active-duty Russian military forces (Lauder, 2018a). However, the Russian government denials served their purpose, which was to create and maintain a degree of ambiguity about the nature of the conflict.

On 16 September, the Russian political leadership of the Donetsk and Luhansk announced the formation of a single defence force, called the United Armed Forces (UAF) of Novorossiya. The announcement marked the start of (what would become) a long transformation of network of relatively independent Russian militias, controlled by a variety of charismatic leaders who often pursued their own personal agendas and interests, into a well-structured and professional military force with modern equipment and a highly capable command and control system. To

[17] Approximately 40 members of the Night Wolves fought with or alongside Russian militia groups in eastern Ukraine, and at least three members of the biker club were killed in combat (Lauder, 2018b).

reinforce discipline and remove (either through incentives or coercion, such as assassination) more problematic local leadership, the Russian government dispatched a special team of operatives from Wagner, a Russian-based private military corporation (Lauder, 2018a; Giglio, 2019). Within months, many of the local militia leaders were gone; some under mysterious or questionable circumstances. By late 2014, most of the command positions at the battalion-level and above were occupied by active-duty Russian military officers.

Syria (2013-2018)

Unlike some other conflicts in which the employment of proxy forces was recognized – and in some cases, publicly celebrated – by the Russian government, the use of proxies to achieve Russian geopolitical interests in the Syrian civil war remains incredibly fuzzy. In other words, not much is known about involvement of proxies by the Russian government in the Syrian conflict (Tsvetkova, 2017). This is because the Russian government has not publicly acknowledged involvement by its proxies in the conflict and considers most operations (whether conducted by the Russian military or otherwise) to be a state secret. In addition, the Russian government has actively supressed the public release of information about operations in Syria, largely through threats, intimidation, denials and obfuscation. In general, what we do know about the Russian government employment of proxies in Syria is informed by media reporting on operational failures and casualties, as well as occasional public complaints by spouses or relatives of contractors killed in Syria and social media posts by Russian military contractors.

The use of proxies by the Russian government in Syria appears to have developed in two distinct iterations and entirely focused on the provision of combat services. The first iteration involved the deployment of a private security company known as Slavonic Corps, sometimes referred to as SlavCorps. Registered in Hong Kong and associated with the Moran Security Group (another private security company), Slavonic Corps was led by two Russian nationals, Vadim Gusev and Yevgeniy Sidorov (Weiss, 2013). In early 2013,[18] Slavonic Corps advertised employment opportunities promising to pay up to $4000 (US) a month as security contractors on Russian social media platforms and related military blogs and websites (Swenson, 2013). By the end of the summer, Slavonic Corps recruited nearly 270 contractors, most of whom had recent experience in the Russian military or security services, including Airborne, Spetsnaz and special police units (Miller, 2014) (see Figure 2: Members of Slavonic Corps in Syria in 2013). One of Slavonic Corps' most notable, credible and experienced members was Lieutenant Colonel (LCol) Dmitry Utkin, a recently retired Spetsnaz battalion commander.

[18] It should be noted that this was nearly a year prior to the Russian military invasion of Ukraine, and more than two years before the Russian government officially committed troops to Syria.

Most of the members of Slavonic Corps were deployed to Syria by the start of October. Operating out of a Syrian army encampment near Latakia, Slavonic Corps was divided into two company-sized tactical units; the first company was comprised of Kuban Cossacks, and the second company was made up of former military and police members from across Russia (Weiss, 2013).

By mid-October, Slavonic Corps received orders to move-out. However, rather than provide security at oil production facilities far from the fighting, they were asked to conduct raids and clear facilities occupied by various insurgent forces and terrorist groups, approximately 500kms inside rebel-controlled areas (Weiss, 2013). Moreover, many of the members of Slavonic Corps started to suspect their activities in-country may not be conducted on behalf of the Syrian government (specifically, the Ministry of Oil and Mineral Reserves) and sanctioned by the highest levels of the Russian government (or at least approved by the FSB), but rather for private business interests, quite possibly for a local wealthy businessman and a Russian oil and gas corporation (Spearin, 2018; Weiss, 2013; Swenson, 2013; Murtazin, 2018). The uncertainty, however, did not deter the group for stepping-off on the mission, and they departed the Syrian military encampment on 15 October 2013.

On 18 October 2013, the Slavonic Corps convoy, accompanied by Syrian government troops and allied militias, was ambushed near the city of Homs by a sizeable contingent of fighters (numbering between 2,000 and 6,000 men) from Jaysh al-Islam (Weiss, 2013). When contact was reported by one the lead vehicles, one of Slavonic Corps companies quickly dismounted and set-up and all-round defence, while other the other attempted to outflank the insurgent forces. After several hours of fierce fighting, it became clear to the leadership of Slavonic Corps they were getting bogged-down and unable to advance and overcome the numerical advantage of the jihadist forces. As a result, Slavonic Corps and its Syrian allies, using a sand storm as cover, made a hasty retreat to their home base in Latakia (Weiss, 2013; Swenson, 2013).

When it was all over, Slavonic Corps incurred only a handful of injuries (albeit two men suffered serious wounds), but no deaths. However, the reputation of the Russian contractors as a professional fighting force was significantly damaged. Within days, Slavonic Corps had their vehicles and weapons confiscated, which were provided by the Syrian army, and the unit was unceremoniously loaded onto an airplane and returned to Moscow (Weiss, 2013).

The situation, however, went from bad to worse for Slavonic Corps. Upon their arrival in Moscow, the plane was surrounded by a special detachment of FSB agents, and all the contractors were detained (Weiss, 2013). While most were allowed to go free after several hours of interrogation, Gusev and Sidorov were arrested and later charged and convicted under article 359 of the Russian criminal code prohibiting mercenary activities. Both Gusev and

Sidorov received a three-year sentence for the Syrian misadventure, and most of the Slavonic Corps contractors were never paid for their effort (Miller, 2014).

However, reports suggest that, while the Russian leadership in the defence and security community considered the Slavonic Corps a debacle (Weiss, 2013), the idea of a deniable military force was worthy of further investment, especially with numerous conflicts on the horizon, most notably Ukraine. It just needed to be done correctly (i.e., properly directed, financed and equipped), and with the right (i.e., politically connected) people leading the effort (Khazov-Kassia, 2018; Patty, 2018).

Figure 2: Members of Slavonic Corps in Syria in 2013 (Swenson, 2013).

The second iteration of Russian government employment of proxies in Syria involved a private military corporation known as The Wagner Group (or Wagner), which gained significant operational experience in eastern Ukraine. Similar to Slavonic Corps, much of what is known about the employment of Wagner in Syria comes from journalists, often investigating a story about a significant operational failure or Russian civilian casualties, or from the occasional social media post by current or former members. As a result, details about the organization, in particular the types of operations conducted in support of official Russian troops or the Syrian government, are extremely difficult to verify, and much of what is discussed in the media remains – for the most part – conjecture. At least one report indicates Wagner is used as an elite infantry in order to prepare the ground for Russian special forces, as well as forward observers and joint terminal attack controllers (Sharogradsky, Gostev & Krutov, 2016). Another report claims Wagner trained, equipped and conducted operations with a specialized unit of

the Syrian army, known as the ISIS Hunters, which operates as an independent military unit (Kramer, 2017).

Established in 2014 and registered in Hong Kong, Wagner (or, more accurately, the Wagner Group), was co-founded by Dmitry Utkin, a former LCol in the Russian Spetsnaz and member the Slavonic Corps, and Yevgeny Prigozhin, a close friend of Putin and owner of the Internet Research Agency, also known as the Russian troll farm (Dyner, 2018). By October 2015, less than a month after the official deployment of Russian troops, Wagner deployed several hundred members to Syria. Likely due to a series of operational successes, as well as increased pressure on the Russian government to minimise exposure to risk, Wagner steadily grew as an organization, with estimates of between 3,000-6,000 active employees by the end of 2017. According to some reports, Wagner deployed upwards of 1,500 contractors (i.e., two battalions) at one time to Syria.

Although the group was involved in a number of operations in Syria, including significant offensives in Palmyra in 2016 and 2017, and incurred numerous casualties,[19] two incidents stand-out. The first occurred in September 2017 when two members were captured by jihadist soldiers during a Daesh counter-offensive in Deir ez-Zur. Shortly after being captured, Daesh posted a video of the two men, who refused to renounce Christianity and convert to Islam (Stewart, 2017). In response, the Russian government attempted to distance itself from the two captives, stating that while they were most likely Russian citizens, they "were not part of the Russian armed forces (Carroll, 2017)." By early October, it was believed the men were executed by Daesh in a town square, along with a number of other captives (Sudakov, 2017). However, the Russian government has not made a public statement about the status or fate of the two men, other than to publicly state that any operation conducted by the Ministry of Defence in Syria was considered classified.

The second incident occurred on 07 February 2018 when several hundred fighters, backed by artillery and armour, were killed in a botched frontal assault on a small military outpost near Deir ez-Zur occupied by Syrian Democratic Forces (SDF) and a small contingent of US Special Operations Forces (USSOF). While not all the fighters were Wagner employees, it is estimated by several media outlets that upwards of 200 Russian citizens were killed in the counter-attack.

Details about the incident remain unclear. However, what has been substantiated, is that a significant number of unidentified, Russian-speaking and Syrian troops crossed the Euphrates river using military barges over the course of a week and assembled in what was recognized as

[19] Some reports suggest that, between 2015 and 2017, at least 150 Wagner fighters have been killed and nearly 1000 injured in Syria (Rogers, 2018).

the US/Allied area of operations (Giglio, 2019).[20] Concerned about the build-up of troops, which was now battalion-sized, and the threat it presented, US officials responsible for allied operations in the area contacted their Russian counter-parts, who steadfastly denied knowledge of any Russian troops or operations in the area (Anotova & Ezzor, 2018).

On the evening of 07 February, the unidentified troops stepped-off and quickly advanced on the SDF/USSOF outpost. After receiving an initial barrage of artillery and direct fire, USSOF personnel returned fire with anti-tank weapons and called in air-strikes as well as artillery support from a near-by Marine fire-base. The fire-fight lasted for more than three hours, but when it was done, the attacking force was decimated, with casualties numbering in the hundreds and an estimated 100-200 Russian contractors killed (Spearin, 2018). In contrast, SDF and USSOF did not suffer any significant injuries or deaths.

In response to the incident, the Russian government stated that no Russian servicemen were involved, and that a few Russian citizens may have been killed, although the exact citizenship of the deceased had not been determined. Specifically, Dmitry Peskov, Putin's spokesperson, stated to reporters that "Russian private citizens fighting alongside the Syrian army are volunteers … and have nothing to do with the state (Trevithick, 2018)." Maria Zakharova, a spokesperson for the Ministry of Foreign Affairs, referred to the incident, in particular the high number of casualties, as "disinformation (Staff Writer, 2018)." Igor Strelkov, who led pro-Russian forces in eastern Ukraine in 2014, claimed on social media that the US counter-attack completely destroyed two tactical units operated by Wagner (Trevithick, 2018).

Later, the Russian government explained the incident as a mistaken attempt to eliminate a Daesh stronghold and reprimanded the leadership of the Syrian government forces for not coordinating the assault with the Russian military command (Felgenhauer, 2018). However, US authorities regard the claim that local forces operated without Russian command knowledge or consent as disingenuous, and subsequently revealed that, in the week prior to the incident, Prigozhin received permission from top Russian and Syrian officials for the offensive (Luhn, 2018). Moreover, reports suggest that Wagner directly coordinates operations with the Syrian government, and that they have a liaison officer with the Russian command in order to coordinate air and artillery support (Khazov-Kassia, 2018).

While there are some similarities between Slavonic Corps and Wagner, in particular that the bulk of Slavonic Corps members were offered and took up employment with Wagner (Khazov-Kassia, 2018), including LCol Dmitry Utkin, and that payment for service is conducted through

[20] US intelligence, surveillance and reconnaissance assets intercepted communications from the troops, which were speaking Russian.

an interested third-party (Khazov-Kassia, 2018),[21] there is one stark contrast – and that is the direct operational and logistical support Wagner receives from the Russian government, including use of a military base (co-located with the 10th Brigade, GRU Spetsnaz forces) near Krasnodar, Russia, to train and deploy from, as well as military transport aircraft, equipment and weapons.[22] Such a degree of support clearly indicates the close-working relationship between Wagner and the Russian state, namely the Ministry of Defence, something Slavonic Corps did not enjoy.

Since Syria, Wagner has deployed its members on behalf of the Russian government to a number of locations around the world, including Libya, Sudan and the Central African Republic, ostensibly to train local forces and protect oil and gas and mineral extraction infrastructure (Hauer, 2018; Goble, 2018; Dyner, 2018). In the case of Sudan, Wagner employees were transported by Russian military aircraft, which were under contract by M Invest LLC, a St. Petersburg-based company owned by Prigozhin. It was later revealed that M Invest advised the Sudanese government on strategies to subvert political protest movements (Lister, Shukla & Elbagir, 2019). More recently, a sizeable contingent of Wagner employees were deployed with Russian Spetsnaz and government technical staff to Venezuela in an effort to prop-up Nicolas Maduro.

[21] In the case of Wagner, operations and employees are financed and paid by Evro Polis Limited, a Russian oil and gas company associated with Prigozhin (Murtazin, 2018). According to reports, Evro Polish also signed a contract with the Syrian government, which gave it 25% of future oil production for all facilities it was able to secure (Kramer, 2017). In early 2018, Evro Polis was added to the US economic sanctions list.

[22] To help conceal the connection with Wagner, court records refer to the barracks adjacent to a Russian military base and believed to be used as a training and staging centre as a "children's vacation camp." Court records also indicate the site was developed by Megalain, a firm linked to Prigozhin (Sagdiev, Zverev & Tsvetkova, 2019).

Section 3: Russian Proxy Employment Model and Implications for NATO

Before proposing a conceptual model of proxy employment by the Russian government and discussing implications for NATO, one question should be addressed: Why does the Russian government utilize proxies? Although a comprehensive explanation is beyond the remit of this article, there appears to be four reasons for outsourcing defence and security functions to proxies in support of political warfare. The first reason is that proxies provide the Kremlin with relatively easy access to a highly-skilled and specialized work-force, which is currently in short-supply in both government agencies and the military (Lauder, 2018b). The second reason is that the employment of proxies is less expensive than maintaining a robust, organic and permanent specialized force (either in the military or the security services), especially if the cost can be off-set or assumed by interested third-parties, such as corporate entities with commercial interests (e.g., oil and gas extraction, mining, etc.) in a particular geographic region. The third reason is that of casualty aversion (Krieg & Rickli, 2018). In other words, proxies are a convenient alternative to the use of (official) military forces, especially when reporting of casualty rates for the military is a legislated requirement (as in the case of Russia). Although casualty information tends to become public knowledge, typically through disgruntled family members, the Russian government is not legally obligated to publish, or even recognize, casualties incurred by private military contractors or other proxies. The fourth and most compelling reason is that it allows for plausible deniability, which is a central feature of Russia's political warfare construct (Lauder, 2018b). In essence, the employment of proxies provides a degree of separation (i.e., intentionally blurs the line) between the Russian government and activities on the ground (Byman, 2018).

Trends in Proxy Employment

Three broad trends can be identified in the employment of proxies by the Russian government. The first trend is that proxies are playing a leading role in the execution of political warfare. In other words, proxies are moving from merely a support or adjunct role, to that of the protagonist, backed up by regular or institutional forces or government agencies. The second trend is that the role of proxies in the execution of political warfare has expanded significantly over the course of the last decade, from relatively narrow or limited activities to encompassing the full spectrum of activities. The last trend is that of increased professionalization and (ironically) formalization of proxies, in particular those that conduct combat operations in high risk environments. While it may appear contradictory to the objective of maintaining a deniable force presence, the shift towards professionalization and formalization is likely due to the historically unreliable and unpredictable nature of local proxy forces, which often pursue their own political and other interests (Mumford, 2013; Brown, 2016). In other words, the Russian

government is seeking a balance between deniability and reliability, and this may be achieved by developing a professional, albeit private and expendable, cadre of war-fighters.

Conceptual Model of Russian Employment of Proxies

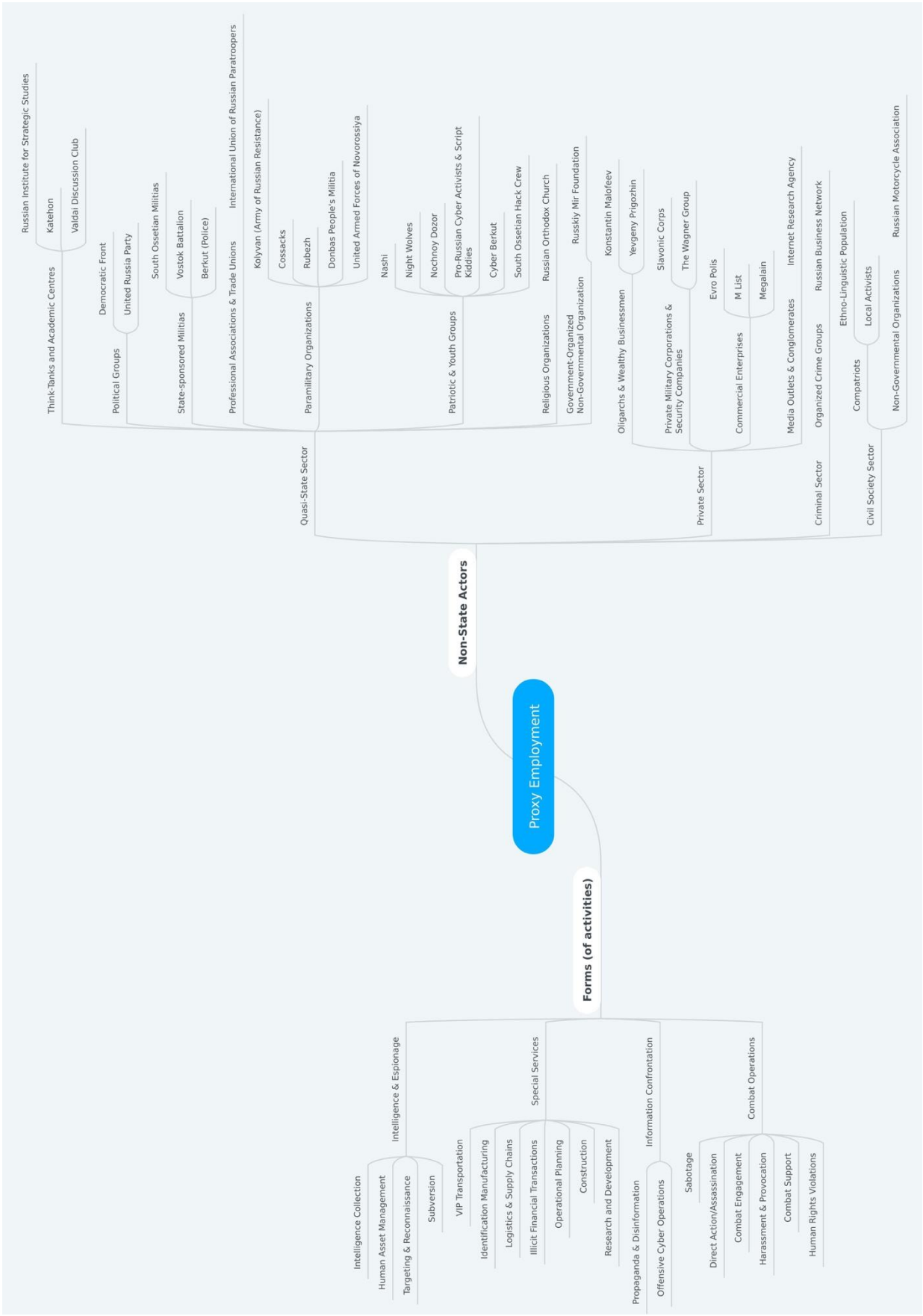
Based upon an examination of Russian strategic doctrine and operational examples from several contemporary conflicts (i.e., Estonia, Georgia, Ukraine and Syria), the following conceptual model for the employment of proxies by the Russian government is proposed (see Figure 3: Conceptual Model of Russian Employment of Proxies). The conceptual model is divided into four *forms of activities* and four general *types of non-state actors*. The first form is that of *special services*, which includes, but is not limited to, operating logistic and supply chains, construction, research and development, illicit financial transactions, operational planning, the manufacture of identity documents, and very important person (VIP) transportation. The second form is that of *intelligence and espionage*, which includes intelligence collection, recruiting and managing human assets, target identification and reconnaissance, and political and social subversion. The third form is that of *information confrontation*, which includes the design and execution of propaganda and disinformation activities using both new and old media, as well as offensive cyber operations. The last form is that of *combat operations*, which includes the execution of campaigns to harass and provoke the enemy, sabotage of critical infrastructure, direct action and assassination, raids and assaults, and other forms of combat engagement (e.g., directing artillery and air-strikes), as well as combat support activities (e.g., mentoring and training, point and personnel security). In some cases, proxies have been used or permitted to conduct human rights violations, such as looting, rape, assault, kidnapping and torture, to intimidate or forcibly remove a local population from a geographic area.

The conceptual model is also divided into four broad categories of non-state actors. The first category is that of *quasi-state sector actors* and includes arms-length or semi-autonomous organizations that are fully or partially funded (or otherwise, such as equipment and materiel) supported by the Russian government. Most state-sponsored militias, such as the Vostok Battalion, and paramilitary organizations, as well as most government-organized non-governmental organizations, fall into this category. The second category is that of *civil society sector*, which includes political and social activists and movements, compatriot groups and most non-governmental organizations. The third category is that of *private sector actors*, such as oligarchs, commercial enterprises and corporations. The last category is that of *criminal sector actors* and includes organized crime groups, crime cartels and other enterprises engaged in illicit activities, including black markets.

Four points should be noted about the conceptual model. First, all conflicts are treated as unique, and the type of proxies employed, and the forms of activities they engage in, are

determined by local socio-political conditions. In other words, there is no template or set framework for the employment of proxies by the Russian government for the purposes of prosecuting political warfare. Second, some proxies engage in blended activities or have subsidiaries or other affiliates that fall across categories. For example, the Night Wolves is a patriotic biker group that operates a series of private businesses, as well as semi-autonomous, non-profit organizations funded by the Kremlin. The Night Wolves is also known to engage in criminal activities, including operating protection rackets, and has a subsidiary organization operating as a private business network (known as Wolf Holdings) that serves not only as a private military corporation, but also conducts research and development and provides a range of technical and paramilitary training services (Lauder, 2018b). In short, the Night Wolves could be assigned to any category of non-state actors, as their structure spans all types of non-state actors. However, for ease of readership, the Night Wolves have been allocated to a single category. Third, there are no clear-lines of demarcation between the forms of activities and how proxies are employed or the services they provide. In other words, proxies may engage in activities spanning one or more forms. In some, albeit rare, circumstances, a proxy may be entrusted by the Russian government to engage in activities spanning all four forms. Lastly, this is evolving space characterized by trial-and-error. In other words, as the Russian government explores the utility of proxies in political warfare, it should be expected that the type of proxies, as well as the forms of activities, will evolve and likely expand over time.

Figure 3: Conceptual Model of Russian Employment of Proxies



Implication to and Recommendations for NATO

The Russian government shows no signs of abating its use of proxies in support of political warfare (Carpenter, 2019; Cole, No Date; Chivvis, 2017; Graja, 2019; Stangl, 2019).[23] At the same time, the execution of and response to political warfare remains a significant doctrinal, capability and policy gap for Western military forces, including NATO (Lauder, 2018a; Fox, 2019). As such, it is likely that the Russian government will not only continue to use a wide-range of proxies to conduct activities but will likely expand and evolve both the type of non-state actors involved as well as the form of activities – in particular for offensive purposes while keeping a conflict under the threshold of war – to achieve geopolitical objectives. The Russian government will also likely seek to professionalize and formalize at least some types of proxies, such as private military corporations (e.g., Wagner), to ensure a high-degree of reliability and operational-control while maintaining a degree of deniability and ambiguity, even if such a separation between the state and proxy is obviously disingenuous (Spearin, 2018).

The implication of Russia's approach to political warfare is that, rather than expanding capabilities specifically for peer-based, high-intensity conflict (i.e., traditional war, which appears to be the current direction of some NATO members) (Weisgerber, 2019), NATO should develop a balanced approach, investing in equipment to prosecute traditional warfare while at the same time developing and expanding policies, doctrine and capabilities for the purposes of planning and conducting political warfare (Carpenter, 2019; Naylor, 2018; Stangl, 2019). This includes, but is not limited to, increasing investment in and broadening the mission of NATO special forces and information related capabilities, specifically to operate within a whole-of-government framework and in pre-Phase 0 of operations (Scharre, 2016). This retuning of policy, doctrine and capability development is not only relevant to deterring and responding to Russian aggression, but is applicable to other state-based adversaries, namely China, which has emphasised leveraging all elements of national power to achieve geopolitical objectives and continues to invest in information, space, and cyber capabilities (Office of the Secretary of Defense, 2019).

Based upon the examination of Russian military theorists and capability proponents, strategic doctrine and policy, and recent operational examples of the utilization of proxies in the execution of political warfare, three overlapping recommendations have been identified. The

[23] This is not to say that military measures and violent armed action will not be applied; rather, military measures are applied in support of non-military measures. In other words, it is not one or the other, but rather a blending of both non-military and military measures that, depending upon local conditions, evolves over the course of a conflict (Chivvis, 2017; Kofman, et al., 2017; Stangl, 2019). However, even if military measures and armed violence are utilized, it is done so in such a way (i.e., limited in time and space) that the conflict remains under the threshold of traditional war. In fact, Michael Carpenter (2019) notes that the Russian government recognizes that the use of military force, even when tactically successful, often results in strategic failure.

first recommendation is that NATO should rethink the value of maintaining traditional conceptual boundaries, specifically between peace and war, combatant and non-combatant, and tactical, operational and strategic levels of conflict. Alternatively, NATO must explore ways to effectively counter and neutralize Russia's efforts to intentionally obfuscate these conceptual distinctions. The second recommendation is that NATO should examine and implement measures to counter the broad application of proxies and non-military means by the Russian government. While building community awareness and a resilient civil society is a good first step, other protective policies and legal frameworks (i.e., to prevent the use of proxies for offensive purposes), mechanisms and structures should also be explored. For example, international mechanisms for holding political and military leaders accountable for actions of proxies should be investigated and implemented, as a failure to adequately address the issue of responsibility will not only allow Russia to continue employ proxies unchecked but would also allow them to expand the use of proxies in future conflicts (Hanlon, 2018). This also includes the development of intelligence capabilities to help identify the use of proxies, especially in conflicts that remain under the threshold of war (Carpenter, 2019; Chivvis, 2017; Treverton, 2019). The last recommendation is that NATO should examine and implement new deterrence concepts, with a focus on unconventional and non-traditional threats and risk calculations (Flanagan et al., 2019), especially as they related to authoritarian regimes.

Conclusion

Since the late 1990s, the Russian Federation has implemented a comprehensive defence and security sector revitalization program. In addition to the acquisition of new military equipment and capabilities, the revitalization program includes the development of a new operating construct, often referred to as political warfare, which guides the employment of both military and non-military mean to achieve geopolitical objectives. A central feature of Russia's political warfare construct is the utilization of proxies. In fact, proxies are conceived of as the primary protagonists of Russia's approach to political warfare, conducting most of the heavy-lifting with the state services – such as the military and security agencies – playing a coordination and support role. This conceptualization of the central role of proxies is formalized and institutionalized in the broad set of Russian government strategic doctrines and policy. In fact, strategic doctrine and policy clearly identifies the need for the full and active participation of all actors from across the private and public sectors in political warfare. As such, proxies are not limited to private military corporations and security companies, but include the breadth of commercial enterprises, government-organized non-governmental organizations and non-government organizations, as well as professional associations and trade unions, think-tanks and academic centres, religious organizations, political groups, oligarchs, criminal organizations, patriotic groups, and paramilitary organizations and state-sponsored militias. The political warfare construct also seeks to empower and exploit civilian and other forms of non-combatant participation in contemporary interstate conflict, further blurring traditional conceptual boundaries and making it extremely difficult for NATO to respond to Russian aggression.

Although not intended to be a comprehensive examination, the use of proxies by the Russian government in several contemporary interstate conflicts was discussed, namely Estonia (2007), Georgia (2008), Ukraine (2014) and Syria (2013-2018). These conflicts revealed three trends. The first trend is that proxies are increasingly playing a leading role in the execution of political warfare. That is, proxies are moving from a support role (to the Russian military) to that of the primary protagonist, backed up by regular or institutional military forces or government security agencies. The second trend is that the role of proxies in political warfare has expanded significantly over the course of the last decade, from relatively narrowly and limited activities to encompassing the full spectrum of activities. The last trend is that of increased professionalization and formalization of proxies, in particular those that conduct combat operations in high risk environments.

Based upon an examination of Russian strategic doctrine and operational examples, the following a conceptual model for the employment of proxies by the Russian government is proposed. The conceptual is divided into four forms of activities (i.e., special services,

intelligence and espionage, information confrontation, and combat operations) and four general types of non-state actors (i.e., quasi-state sector, civil society sector, private sector, and criminal sector).

Three recommendations for NATO are also proposed, namely the requirement to rethink the value of traditional conceptual boundaries, implement counter-measures to Russian application of proxies and non-military measures, and to research, validate and implement new deterrence concepts with a focus on unconventional and non-traditional threats.

Whereas NATO focused on the development of capabilities to conduct counter-terrorism and counter-insurgency operations in the intermediate post-Cold War era, the Russian Federation invested in and modernized its political warfare capability. As a result of testing and implementing new organizational structures, policies, doctrine and tactics, and embracing new technology (e.g., electronic warfare, cyber, social media and mobile technology) and proxies as a force multiplier and intentionally manipulating and blurring traditional distinctions conceptual distinctions between peace and war and combatant and non-combatant, the Russian government achieved an asymmetric advantage over NATO.

References

Anotova, M. & Ezzor, D. (2018, February 17). Russian mercenaries, a secretive weapon in Syria. *The Times of Israel.* Retrieved from: https://www.timesofisrael.com/russian-mercenaries-a-discrete-weapon-in-syria/

Arbatov, A. (2000, July). The transformation of Russian military doctrine: Lessons learned from Kosovo and Chechnya. *The Marshall Center*. Retrieved from: https://apps.dtic.mil/dtic/tr/fulltext/u2/a478927.pdf

Army of Russian Resistance. (2007, June 29). Army of Russian resistance calls on Putin to introduce troops to Estonia. Message posted to https://general-ivanov.livejournal.com/43163.html

Baezner, M. (2018, October). Hotspot analysis: Cyber and information warfare in the Ukrainian conflict (version 2). Centre for Security Studies: Zurich. Retrieved from: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf

Barabanov, M. (2015). Viewing the action in Ukraine from the Kremlin's Window. In C. Howard & R. Pukhov, *Brothers armed: Military aspects of the crisis in Ukraine (2nd Edition)* (pp. 187-201). Minneapolis: East View Press.

Barabanov, M., Lavrov, A., Pukhov, R., & Tseluiko, V. (2010). The tanks of August. *Centre for Analysis of Strategies and Technologies.* Retrieved from: http://www.cast.ru/files/The_Tanks_of_August_sm_eng.pdf

Barnard, A. (2008, August 09). Georgia and Russia nearing all-out war. *The New York Times.* Retrieved from: https://www.nytimes.com/2008/08/10/world/europe/10georgia.html?_r=1&partner=rssuserland&emc=rss&pagewanted=all&oref=slogin

Barry, E. & Schwirtz, M. (2009, April 06). Killing of leader's foes may test Kremlin's will. *The New York Times.* Retrieved from: https://www.nytimes.com/2009/04/07/world/europe/07chechnya.html?mtrref=undefined&gwh=28FA719F27BBA19E35581950C168B21D&gwt=pay

Beehner, L., Collins, L., Ferenzi, S., Person, R., & Brantly, A. (2018, March 20). Analyzing the Russian way of war: Evidence from the 2008 conflict with Georgia. *Modern War Institute.*

Retrieved from: https://mwi.usma.edu/analyzing-russian-way-war-evidence-2008-conflict-georgia/

Bender, J. (2015, January 12). Russia's new military doctrine shows Putin's geopolitical ambitions. *Business Insider.* Retrieved from: https://www.businessinsider.com/russia-has-a-new-military-doctrine-2015-1

Blank, S. (2008). Web War I: Is Europe's first information war a new kind of war? *Comparative Strategy,* (27(3), Retrieved from: https://doi.org/10.1080/01495930802185312

Bondarenko, M. & Sas, I. (2008, August 08). Shawls bald. *Nezavisimaya Gazeta.*

Brown, S. (2016). Purpose and pitfalls of war by proxy: A systemic analysis. *Small Wars and Insurgencies.* 27(2). Retrieved from: https://doi.org/10.1080/09592318.2015.1134047

Byman, D.L. (2018, May 21). Why engage in proxy war? A state's perspective. *Brookings Institute.* Retrieved from: https://www.brookings.edu/blog/order-from-chaos/2018/05/21/why-engage-in-proxy-war-a-states-perspective/

Carpenter, M. (2019, May 29). Countering Russia's malign influence operations. *Just Security.* Retrieved from: https://www.justsecurity.org/64327/countering-russias-malign-influence-operations/

Carroll, O. (2017, October 04). Kremlin distances itself from captured 'Russian soldiers' shown in ISIS propaganda video. *The Independent.* Retrieved from: https://www.independent.co.uk/news/world/europe/isis-russia-video-soldiers-syria-kremlin-mercenaries-roman-zabolotny-grigory-tsurkanu-a7983316.html

Cavegn, D. (2017, June 26). Ansip, Laaneots: Russian agents present during Bronze Night riots. *EER.* Retrieved from: https://news.err.ee/592127/ansip-laaneots-russian-agents-present-during-bronze-night-riots

Chausovsky, E. (2018m, August 07). Looking back on the Russian-Georgian war, 10 years later. *Stratfor.* Retrieved from: https://worldview.stratfor.com/article/looking-back-russian-georgian-war-10-years-later

Chivers, C.J. (2008, September 15). Georgia offers fresh evidence on war's start. *The New York Times.* Retrieved from: https://www.nytimes.com/2008/09/16/world/europe/16georgia.html

Chivers, C.J. & Barry, E. (2008, November 06). Georgia claims on Russia war called into question. *The New York Times.* Retrieved from: https://www.nytimes.com/2008/11/07/world/europe/07georgia.html

Chivvis, C.S. (2017, March 22). Understanding Russian "hybrid warfare:" And what can be done about it. *RAND.* Retrieved from: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

Clover, C., Belton, C., Dombey, D., & Cienski, J. (2008, August 26). Countdown in the Caucasus: Seven days that brought Russia and Georgia to war. *Financial Times.* Retrieved from: https://www.ft.com/content/af25400a-739d-11dd-8a66-0000779fd18c

Cole, R. (No Date). The myths of traditional warfare: How our peer and near-peer adversaries plan to fight using irregular warfare. *Small Wars Journal.* Retrieved from: https://smallwarsjournal.com/jrnl/art/myths-traditional-warfare-how-our-peer-and-near-peer-adversaries-plan-fight-using

Connell, M., & Vogler, S., (2017, March). Russia's approach to cyber warfare. *CNA.* Retrieved from: https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

Council of the European Union. (2009, September). *Independent international fact-finding mission on the conflict in Georgia*. Retrieved from: https://www.echr.coe.int/Documents/HUDOC_38263_08_Annexes_ENG.pdf

Covoli, I. (2014, December 27). Russia's revised military doctrine sees major threats from NATO, US. *VOA.* Retrieved from: https://www.voanews.com/a/russia-identifies-nato-us-as-major-threats/2574605.html

Danchev, D. (2008, August 11). Coordinated Russia vs Georgia cyber attacks in progress. *Zero Day.* Retrieved from: https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/

Darczewska, J. (2016, June 27). Russia's armed forces on the information war front: Strategic documents. *Centre for Easter Studies, 57.* Retrieved from: http://aei.pitt.edu/78572/1/prace_57_ang_russias_armed_forces_net.pdf. Accessed: 01 February 2019.

Davis, J. (2007, August 21). Hackers take down the most wired country in Europe. *Wired.* Retrieved from: https://www.wired.com/2007/08/ff-estonia/

Dyner, A.M. (2017, January 05). The Russian Federation's new foreign policy concept. *Australian Institute of International Affairs*. Retrieved from: http://www.internationalaffairs.org.au/global-wire/the-russian-federations-new-foreign-policy-concept/

Dyner, A.M. (2018, May 04). The role of private military contractors in Russian foreign policy. *The Polish Institute of International Affairs,* 64(1135). Retrieved from: http://www.pism.pl/publications/bulletin/no-64-1135

Dzhindzhikhashvili, M. (2008, August 10). Russia expands Georgia blitz, deploys ships. *Yahoo News.* Retrieved from: http://news.yahoo.com/s/ap/20080810/ap_on_re_eu/georgia_south_ossetia

Ermus, A. & Salum, K. (2017, July). Changing concepts of war: Russia's new military doctrine and the concept of hybrid warfare. In V. Sazonov, K. Muur, H. Molder, and A. Saumets (Eds)., *Russian Information Warfare Against the Ukrainian State and Defence Forces: April-December 2014.* Retrieved from: https://www.ksk.edu.ee/wp-content/uploads/2017/02/Report_infoops_08.02.2017.pdf

European Parliament. (2017). Russia's national security strategy and military doctrine and their implications for the EU. *European Parliament*. Retrieved from: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/578016/EXPO_IDA%282017%29578016_EN.pdf

Felgenhauer, P. (2018, February 15). Death of military contractors illuminates Russia's war by proxy in Syria. *Eurasia Daily Monitor,* 15(24). Retrieved from: https://jamestown.org/program/death-military-contractors-illuminates-russias-war-proxy-syria/

Finn, P. (2008, August 17). A two-sided descent into full-scale war. *Washington Post.* Retrieved from: http://www.washingtonpost.com/wp-dyn/content/article/2008/08/16/AR2008081600502_pf.html?noredirect=on

Flanagan, S.J., Osburg, J., Binnendijk, A., Kepe, M., & Radin, A. (2019). Deterring Russian aggression in the Baltic States through resilience and resistance. *RAND.* Retrieved from: https://www.rand.org/pubs/research_reports/RR2779.html

Fox, A.C., (2019, March-April). Time, power, and the principal-agent problems: Why the US Army is ill-suited for proxy warfare hotspots. *Military Review.* https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/28-Time-Power/

Giglio, M. (2019, April 17). Inside the shadow war fought by Russian mercenaries. *Buzzfeed News.* Retrieved from: https://www.buzzfeednews.com/article/mikegiglio/inside-wagner-mercenaries-russia-ukraine-syria-prighozhin

Giles, K. (2016, March). Russia's 'new' tools for confronting the West: Continuity and innovation in Moscow's exercise of power. *Chatham House*. Retrieved from: https://www.chathamhouse.org/sites/default/files/publications/2016-03-russia-new-tools-giles.pdf. Accessed: 01 February 2019.

Goble, P. (2018, November 15). Russian nationalist group, acting as private military company, worries Kremlin. *Eurasia Daily Monitor,* 15(164). Retrieved from: https://jamestown.org/program/russian-nationalist-group-acting-as-a-private-military-company-worries-kremlin/

Government of Russia. (2000a, January 10). National security concept of the Russian Federation. *Government of the Russian Federation*. Retrieved from: http://www.mid.ru/en/web/guest/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768

Government of Russia. (2000b, April 21). On approval of the military doctrine of the Russian Federation. *Government of the Russian Federation*. Retrieved from: http://kremlin.ru/acts/bank/15386

Government of Russia. (2000c, June 28). The foreign policy concept of the Russian Federation. *Government of the Russian Federation*. Retrieved from: https://fas.org/nuke/guide/russia/doctrine/econcept.htm

Government of Russia. (2000d, September 09). Information security doctrine of the Russian Federation. *Government of the Russian Federation*. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

Government of Russia. (2011). Conceptual views on the activities of the armed forces of the Russian Federation in the information space. *Government of the Russian Federation*. Retrieved from: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle

Government of Russia. (2014, March 04). Vladimir Putin answered journalists' questions on the situation in Ukraine. *Government of the Russian Federation*. Retrieved from: http://en.kremlin.ru/events/president/news/20366

Government of Russia. (2015a, June 29). The military doctrine of the Russian Federation. *Government of the Russian Federation*. Retrieved from: https://rusemb.org.uk/press/2029

Government of Russia. (2015b, December 31). Russian national security strategy. *Government of the Russian Federation*. Retrieved from: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf

Government of Russia. (2016a, December 01). Foreign policy concept of the Russian Federation. *Government of the Russian Federation*. Retrieved from: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248

Government of Russia. (2016b, December 05). Doctrine of information security of the Russian Federation. *Government of the Russian Federation*. Retrieved from: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

Graja, C. (2019, May). SOF and the future of global competition. *CNA*. Retrieved from: https://www.cna.org/CNA_files/PDF/DCP-2019-U-020033-Final.pdf

Hanlon, B. (2018, February 16). Weak US response to Russian proxies undermines deterrence in Middle East and Eastern Europe. *Institute for the Study of War.* Retrieved from: http://iswresearch.blogspot.com/2018/02/weak-us-response-to-russian-proxies.html

Harding, L. (2008, September 01). Russia's cruel intention. *The Guardian.* Retrieved from: https://www.theguardian.com/commentisfree/2008/sep/01/russia.georgia

Harding, L. & Meikle, J. (2008, August 13). Georgian villages burned and looted as Russian tanks advance. *The Guardian.* Retrieved from: https://www.theguardian.com/world/2008/aug/13/georgia.russia6

Hauer, N. (2018, August 27). Russia's favorite mercenaries. *The Atlantic.* Retrieved from: https://www.theatlantic.com/international/archive/2018/08/russian-mercenaries-wagner-africa/568435/

Iasiello, E.J., (2017). Russia's improved information operations: From Georgia to Crimea. *Parameters,* 47(2). Retrieved from: https://ssi.armywarcollege.edu/pubs/parameters/issues/Summer_2017/8_Iasiello_RussiasImprovedInformationOperations.pdf

Jones, R.C. (No Date). Deterring "Competition short of war": Are Gray Zones the Ardennes of our Modern Maginot Line of Traditional Deterrence? *Small Wars Journal*. Retrieved from:

https://smallwarsjournal.com/jrnl/art/deterring-competition-short-war-are-gray-zones-ardennes-our-modern-maginot-line

Keating, J. (2010, December 07). Who was behind the Estonia cyber attacks? *Foreign Policy.* Retrieved from: https://foreignpolicy.com/2010/12/07/who-was-behind-the-estonia-cyber-attacks/

Keizer, G. (2008, August 11). Cyberattacks knock out Georgia's internet presence. *Computerworld.* Retrieved from: https://www.computerworld.com/article/2532289/cyberattacks-knock-out-georgia-s-internet-presence.html

Khazov-Kassia, S. (2018, March 07). The project "Meat grinder". Three commanders of "PMC Wagner." Radio Liberty. Retrieved from: https://www.svoboda.org/a/29084090.html1/10SYRIATheproject

Kofman, M., Migacheva, K. Nichiporuk, B., Radin, A., Tkacheva, O., & Oberholtzer, J. (2017). Lesson's from Russia's Operations in Crimea and Eastern Ukraine. *RAND.* Retrieved from: https://www.rand.org/pubs/research_reports/RR1498.html

Georgian war. *War on the Rocks.* Retrieved from: https://warontherocks.com/2018/08/the-august-war-ten-years-on-a-retrospective-on-the-russo-georgian-war/

Kofman, M. (2018b, September 04). Russian performance in the Russo-Georgian war revisited. *War on the Rocks.* Retrieved from: https://warontherocks.com/2018/09/russian-performance-in-the-russo-georgian-war-revisited/

Kozey, W. (2017, March 23). Compatriots without borders: Analysis of Russian/pro-Russian government organized non-governmental organizations (GONGO) specific to the conflict in Ukraine, DRDC-RDDC-2017-L096, Scientific Letter. *Defence Research and Development Canada.*

Kramer, A.E. (2017, July 05). Russia deploys a potent weapon in Syria: The profit motive. *The New York Times.* Retrieved from: https://www.nytimes.com/2017/07/05/world/middleeast/russia-syria-oil-isis.html

Krieg, A. & Rickli, J-M. (2018). Surrogate warfare: The art of war in the 21st Century? *Defence Studies,* 18(2), Retrieved from: https://doi.org/10.1080/14702436.2018.1429218

Kureev, A. (2016, December 06). Decoding the changes in Russia's new foreign policy concept. *Russia Direct.* Retrieved from: https://russia-direct.org/opinion/decoding-changes-russias-new-foreign-policy-concept

Kuzio, T. (2017). *Putin's war against Ukraine*. Toronto: CreateSpace.

Lauder, M.A. (2014, November 14). Truth is the first casualty of war: A brief examination of Russian Informational Conflict during the 2014 crisis in Ukraine, DRDC-RDDC-2014-L262, Scientific Letter. *Defence Research and Development Canada*.

Lauder, M.A. (2016, November 30). Iron fist in a velvet glove: A brief examination of the Russian military operation to annex Crimea in 2014, DRD-RDDC-2016-L414, Scientific Letter. *Defence Research and Development Canada.*

Lauder, M.A. (2018a, May). Masters of chaos: The application of political warfare by the Russian Federation in the contemporary operating environment, DRDC-RRDC-2018-L118, Scientific Letter. *Defence Research and Development Canada.*

Lauder, M.A. (2019, May). Gunshots by computers: An examination of Russian information confrontation in doctrine, theory and practice, DRDC-RDDC-2019-D037, Reference Document. *Defence Research and Development Canada.*

Lavrov, S. (2016, March 30). Russia's foreign policy in a historical perspective. *Russia in Global Affairs, 2(135)*. Retrieved from: https://eng.globalaffairs.ru/number/Russias-Foreign-Policy-in-a-Historical-Perspective-18067.

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

Lister, T., Shulka, S., & Elbagir, N. (2019, April 25). Fake news and public executions: Documents show a Russian company's plan for quelling protests in Sudan. *CNN.* Retrieved from: https://edition.cnn.com/2019/04/25/africa/russia-sudan-minvest-plan-to-quell-protests-intl/index.html?no-st=1556190353

LoGiurato, B. (2014, April 17). Putin finally admits to sending troops to Crimea. *Business Insider.* Retrieved from: http://www.businessinsider.com/putin-admits-troops-crimea-2014-4

Luhn, A. (2018, February 23). Russian mercenary boss spoke with Kremlin before attacking US forces in Syria, intel claims. *The Telegraph.* Retrieved from: https://www.telegraph.co.uk/news/2018/02/23/russian-mercenary-boss-spoke-kremlin-attacking-us-forces-syria/

Makarechi, K. (2014, April 17). Vladimir Putin admits Russian troops have been active in Crimea. *Vanity Fair.* Retrieved from: https://www.vanityfair.com/news/politics/2014/04/putin-admits-russian-troops-crimea

Markoff, J. (2008, August 12). Before the gunfire, cyberattacks. *The New York Times.* Retrieved from: https://www.nytimes.com/2008/08/13/technology/13cyber.html

McDermott, R. (2016, January 12). Russia's 2015 national security strategy. *Eurasia Daily Monitor, 13(7).* Retrieved from: https://jamestown.org/program/russias-2015-national-security-strategy/

McGeady, T.D. (2017). *Outsourced Combatants: The Russian State and the Vostok Battalion* (Unplublished Master's Thesis). Virginia Polytechnic Institute and State University, Blacksburg, Virginia.

Meikle, J. & Traynor, I. (2008, August 15). Condoleezza Rice visits Georgia over South Ossetia conflict. *The Guardian.* Retrieved from: https://www.theguardian.com/world/2008/aug/15/georgia.russia

Meyers, S.L. (2007, April 27). Russia rebukes Estonia for moving Soviet statue. *The New York Times.* Retrieved from: https://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html

Miller, J. (2014, January 25). The insane story of Russian mercenaries fighting for the Syrian regime. *Huffington Post.* Retrieved from: https://www.huffpost.com/entry/the-insane-story-of-russi_b_4317729

Monaghan, A. (2013, April). The new Russian foreign policy concept: Evolving continuity. *Chatham House*. Retrieved from: https://www.chathamhouse.org/sites/default/files/public/Research/Russia%20and%20Eurasia/0413pp_monaghan.pdf.

Moses, A. (2008, August 12). Georgian websites forced offline in 'cyber war'. *The Sydney Morning Herald.* Retrieved from: https://www.smh.com.au/technology/georgian-websites-forced-offline-in-cyber-war-20080812-gdsqac.html

Mumford, A. (2013). Proxy warfare and the future of conflict. *The RUSI Journal.* 158(2). Retrieved from: https://doi.org/10.1080/03071847.2013.787733

Murtazon, Y. (2018, January 21). Serve the fatherland! Expensive. *Novaya Gazeta.* Retrieved from: https://www.novayagazeta.ru/articles/2018/01/21/75221-sluzhu-otechestvu-dorogo

Myers, S.L. (2008, August 13). Bush, sending aid, demands that Moscow withdraw. *The New York Times.* Retrieved from: https://www.nytimes.com/2008/08/14/world/europe/14georgia.html

Naylor, S.D. (2018, October 30). After years of fighting insurgencies, the Army pivots to training for a major war. *Yahoo News.* Retrieved from: https://www.yahoo.com/news/years-fighting-insurgencies-army-pivots-training-major-war-090042200.html

Norberg, J. (2014, March 13). *The use of Russia's military in the Crimean crisis*. Carnegie Endowment for International Peace. Retrieved from http://carnegieendowment.org/2014/03/13/use-of-russia-s-military-in-crimean-crisis-pub-54949 1/

Office of the Secretary of Defense. (2019, May 02). Annual report to Congress: Military and security developments Involving the People's Republic of China 2019. *Department of Defense*. Retrieved from: https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf

Oliker, O. (2016, January 07). Unpacking Russia's new national security strategy. *Centre for Strategic and International Studies*. Retrieved from: https://www.csis.org/analysis/unpacking-russias-new-national-security-strategy.

Pallin, C.V., & Westerlund, F. (2009). Russia's war in Georgia: Lessons and consequences. *Small Wars & Insurgencies,* 20(2). Retrieved from: https://doi.org/10.1080/09592310902975539

Patty, B. (2018, February 19). Russia and Syria. War and proxy war. *Security Studies Group.* Retrieved from: https://securitystudies.org/russia-syria-war-proxy-war/

Pynnoniemi, K. (2018). Russia's national security strategy: Analysis and conceptual evolution, *The Journal of Slavic Military Studies, 31(2)*. Retrieved from: https://doi.org/10.1080/13518046.2018.1451091

Rogers, S. (2018, February 01). A Russian Blackwater? Putin's secret soldiers in Ukraine and Syria. *Daily Beast.* Retrieved from: https://www.thedailybeast.com/a-russian-blackwater-putins-secret-soldiers-in-ukraine-and-syria

Ruiz, M.M. (2017, August). A shift in doctrine. *Diplomaatia, 168*. Retrieved from: https://www.diplomaatia.ee/en/article/a-shift-in-russian-doctrine/.

Rutherford, M. (2009, August 19). Report: Russian mob aided cyberattacks on Georgia. *C/Net*. Retrieved from: https://www.cnet.com/news/report-russian-mob-aided-cyberattacks-on-georgia/

Ruus, K. (2008). Cyber War: Estonia attacked from Russia. *European Affairs,* 9(1-2). Retrieved from: https://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia

Sagdiev, R., Zverev, A., & Tsvetkova, M. Exclusive: Kids' camp on a defense base? How Russian firms masked secret military work. *Reuters.* Retrieved from: https://www.reuters.com/article/us-mideast-crisis-syria-russia-prigo…se-base-how-russian-firms-masked-secret-military-work-idUSKCN1RG1QT

Sakwa, R. (2016). Frontline Ukraine: Crisis in the Borderlands. London: I.B. Tauris.

Scharre, P. (2016, October 06). American strategy and the six phases of grief. *War on the Rocks.* Retrieved from: https://warontherocks.com/2016/10/american-strategy-and-the-six-phases-of-grief/

Shachtman, N. (2009, March 11). Kremlin kids: We launched the Estonian cyber war. *Wired.* Retrieved from: https://www.wired.com/2009/03/pro-kremlin-gro/

Shakarian, P. (2011, November-December). The 2008 Russian cyber campaign against Georgia. *Military Review.* Retrieved from: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20111231_art013.pdf

Shargradsky, A., Gostev, A., & Krutov, M. (2016, March 29). Syrian losses of "Slavic Corps." *Radio Liberty.* Retrieved from: https://www.svoboda.org/a/27642396.html

Sherr, J. (2017). The militarization of Russian policy. *Transatlantic Academy, 10*. Retrieved from: https://euagenda.eu/upload/publications/untitled-135828-ea.pdf

Sinovets, P. & Renz, B. (2015, July). Russia's 2014 military doctrine and beyond: Threat perceptions, capabilities and ambitions. *NATO Defence College, 117.* Retrieved from: http://www.ndc.nato.int/news/news.php?icode=830

Spearin, C.R., (2018, Summer). Russia's military and security privatization. *Parameters.* 48(2). Retrieved from: https://ssi.armywarcollege.edu/pubs/parameters/issues/Summer_2018/7_Spearin.pdf

Stangl, M. (2019, May 13). Russia won't start a (conventional) war in the Baltics. *The National Interest.* Retrieved from: https://nationalinterest.org/blog/buzz/russia-wont-start-conventional-war-baltics-57317

Staff Writer. (2008, August 05). 300 volunteers from North Ossetia arrived in Tskhinvali. *Lenta.* Retrieved from: https://lenta.ru/news/2008/08/04/volunteers/

Staff Writer. (2018, February 15). Moscow: Five Russian fighters may have been killed in US strikes in Syria. *Radio Free Europe / Radio Liberty.* Retrieved from: https://www.rferl.org/a/russia-five-russian-fighters-killed-syria-air-strikes-united-states/29041741.html

Steele, J. (2009, February 01). Georgians who can never go home. *The Guardian.* Retrieved from: https://www.theguardian.com/world/2009/feb/01/georgian-refugees-south-ossetia

Stewart, W. (2017, October 06). Russian mercenaries captured by ISIS 'are executed after refusing to reject Christianity and become Muslim'. *Daily Mail.* Retrieved from: https://www.dailymail.co.uk/news/article-4955614/Two-Russian-mercenaries-executed-ISIS.html

Sudakov, D. (2017, October 10). ISIL terrorists take two Russians captive, film and execute them. *Pravda.* Retrieved from: http://www.pravdareport.com/hotspots/138880-isil_terrorists_russians/

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

Swenson, M. (2013, November 18). There are Russian mercenaries fighting in Syria. *War is Boring.* Retrieved from: https://warisboring.com/there-are-russian-mercenaries-fighting-in-syria/

Tabor, D. (2015, October 08). Putin's angels: Inside Russia's most infamous motorcycle club. *RollingStone.* Retrieved from: https://www.rollingstone.com/culture/culture-news/putins-angels-inside-russias-most-infamous-motorcycle-club-56360/

Torchia, C. (2008, August 17). Russia: Will begin pullout from Georgia on Monday. *Yahoo News.* Retrieved from: https://news.yahoo.com/s/ap/20080817/ap_on_re_eu/georgia_russia

Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian.* Retrieved from: mhttps://www.theguardian.com/world/2007/may/17/topstories3.russia

Turovsky, D. (2018, August 07). 'It's our time to serve the Motherland': How Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers. *Meduza.* Retrieved from: https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland

Trenin, D. (2014, December 29). 2014: Russia's new military doctrine tells it all. *Carnegie.* Retrieved from: https://carnegie.ru/commentary/57607

Treverton, G.F., et al. (2018, May). Addressing hybrid threats. *Hybrid COE.* Retrieved from: https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf

Trevithick, J. (2017, September 26). New US Army manual shows It's worries about Russia's hybrid warfare tactics. *The Drive.* Retrieved from: https://www.thedrive.com/the-war-zone/14647/new-us-army-manual-shows-its-worried-about-russias-hybrid-warfare-tactics

Trevithick, J. (2018, February 15). Russian mercenaries take the lead in attacks on US and allied forces in Syria. *The Drive.* Retrieved from: https://www.thedrive.com/the-war-zone/18533/russian-mercenaries-take-a-lead-in-attacks-on-us-and-allied-forces-in-syria

Troeder, E. (2019, May). A whole-of-government approach to gray zone warfare. *Strategic Studies Institute.* Retrieved from: https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1411

Tsvetkova, M. (2017, August 02). Exclusive: Russian losses in Syria jump in 2017, Reuters estimates show. *Reuters.* Retrieved from: https://www.reuters.com/article/us-mideast-crisis-syria-russia-casua…n-losses-in-syria-jump-in-2017-reuters-estimates-show-idUSKBN1AI0HG

van Herpen, M.H., 2015, Putin's wars: The rise of Russia's new imperialism (2nd Edition), Rowman and Littlefield, Lanham.

Weiss, M. (2013, November 21). The case of the keystone Cossacks. *Foreign Policy.* Retrieved from: https://foreignpolicy.com/2013/11/21/the-case-of-the-keystone-cossacks/

Weisgerber, M. (2019, April 16). Army secretary reveals weapons wishlist for war with China & Russia. *Defense One*. Retrieved from: https://www.defenseone.com/business/2019/04/army-secretary-reveals-weapons-wishlist-war-china-russia/156347/

White, S.P. (2018, March 20). Understanding cyberwarfare: Lessons from the Russia-Georgia war. *Modern War Institute.* Retrieved from: https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/

Zevelev, I. (2016, December 12). Russian national identity and foreign policy. *Centre for Strategic and International Studies*. Retrieved from: https://www.csis.org/analysis/russian-national-identity-and-foreign-policy