The Dark Mirror: Gerasimov’s Hybrid War in Ukraine

Citation

Permanent link
https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37365418

Terms of Use
This article was downloaded from Harvard University’s DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA

Share Your Story
The Harvard community has made this article openly available. Please share how this access benefits you. Submit a story.

Accessibility
The Dark Mirror:
Gerasimov’s Hybrid War in Ukraine

Caleb Newton

A Thesis in the Field of International Relations
for the Degree of Master of Liberal Arts in Extension Studies

Harvard University
November 2018
Abstract

This thesis investigates to what extent General Valery Gerasimov’s “hybrid” warfare approach is being used in Russia’s military intervention in Ukraine. Much debate over exactly what is Russia’s strategy in Ukraine is ongoing and Gerasimov’s exact influence on it. This thesis discusses the approach Gerasimov advocates in terms of Russian cyberwarfare, influence campaigns and broader dynamics, such as the competition between civilian and military intelligence in Russia. General Gerasimov’s position as Chief of the General Staff of the Armed Forces of the Russian Federation and First Deputy Minister of Defense of the Russian Federation, his closeness to the highly influential Defense Minister Sergei Shoigu and his willingness to argue for the modernization of the Russian military in a way that uses advanced low cost and high impact hybrid war techniques make it likely that he is and will continue to highly influence Russian military approaches in Ukraine and elsewhere. As a method to counter Gerasimov’s hybrid war techniques, this thesis proposes a de-escalation strategy that interferes with Russian information manipulation and also reduce violence that could escalate to a minimum.
Table of Contents

List of Figures .................................................................................................................. v

Chapter I. Introduction to the Research ............................................................................. 1
  Research Problem ........................................................................................................ 6
  Research Proposition .................................................................................................... 7

Chapter II. Gerasimov’s Information War .......................................................................... 8

Chapter III. Russian Cyberwarfare and Gerasimov .......................................................... 41

Chapter IV. Gerasimov’s Importance ............................................................................... 61

Chapter V. Countering Gerasimov through De-Escalation ............................................. 76

Chapter VI. Conclusions .................................................................................................. 84

References ....................................................................................................................... 87
List of Figures

Figure 1. Value of the Russian Ruble through 2015.............................................14

Figure 2. A Graphical Representation of Gerasimov’s Proposed Approach to Hybrid Warfare Based on Western Color Revolutions..................................................34-5

Figure 3. Gerasimov Presentation to the 2017 Moscow Conference on International Security..........................................................42

Figure 4. Cholera Epidemic and Violence in Chicago (Slutkin, 2013) Compared with an OSCE Map of Civilian Casualties in Eastern Ukraine (OSCE, 2017) .........................82
Ironically, it would be in a hotel named after a famous North American frontiersman Pierre-Espirit Radisson—the Radisson Hotel in Moscow—in a security conference shortly after the Euromaidan revolution in Ukraine that General Valery Gerasimov would outline his strategy to strike back at the West’s continued interference in international affairs—especially in the states that it felt were in the Russian sphere of influence (Cordesman, 2017). The Chief of the General Staff of the Armed Forces and First Deputy Minister of Defense of the Russian Federation had published his now famous speech from the conference the year before in the article *The Value of Science is in the Foresight* in 2013 roughly a year before the government of Ukraine fell, where he clearly argued Russia should turn the color revolution (which he saw as a method of war) into a Russian method of war; in other words, Russia should wage wars in the same “hybrid” fashion he saw the west fighting their “wars”—e.g. color revolution coups (Gerasimov, 2016b; Bartles, 2016). Gerasimov’s articulation of this principle in this article eventually led to this approach being called the “Gerasimov Doctrine” by (Galeotti, 2018).

In that hotel conference, Gerasimov argued for a multipolar world with spheres of influence and that Russia itself use color revolutions as a guide for waging low cost, destabilizing wars around the world (Cordesman, 2017, p. 12-13). It appears Russia has followed the advice of the Chechen war hardened general. President Trump’s former National Security Adviser General H.R. McMaster noted that democracies around the
world are under attack: “We’ve seen that this is really a sophisticated effort to polarize democratic societies and pit communities within those societies against each other” (Garcia & Torres, 2018). Although some claim this is simply a revival of cold war political warfare, this view ignores Russian military thinkers like Gerasimov and wishes to understand post-Soviet Russian information warfare as merely an antiquarian rebirth of the Soviet propaganda and information manipulation that preceded it. Modern Russian information warfare is a combination of the parallel and entwined developments of the Russian economic and political system. Gerasimov’s approach is the logical extension of these developments and Russian military approaches and theories—such as the deep operation theory advanced by Georgy Isserson who he quotes in The Value of Science is in the Foresight (Gerasimov, 2016b).

The Russian economy—much like Gerasimov’s vision of the future of Russian warfare—is a dark reflection of Western systems they tried to implement there. After the collapse of the Soviet Union, Russia embraced the market in a chaotic and haphazard manner that turned the tightly controlled Soviet economic space into a free-for-all; determined to ensure Russia could never return to communism, free marker reformers subjected the Russian economy to “shock therapy”—a process that led to massive inflation and the concentration of formerly state owned resources into the hands of a few—the infamous Oligarchs of Russia (Gustafson, 2012). The lawless form of “capitalism”—a label economist Robert Reich rejected as inappropriate for the Russian system—proved better at fostering criminality than liberalism (Reich, 2001). A whole spam industry designed to troll, spam and promote through comments and fake review arose in Russia (Sanovich, 2017). For a relatively low cost, you could enlist Russians to manipulate the web. Organized crime through very professional sounding entities like the
“Russian Business Network (RBN)” facilitated the “use and lease [of] botnets for various purposes” (Shakarian, 2011). In 2008, the Russians would be one of the first armies in the world to use a Distributed Denial of Service Attack as a weapon of war in their brief war with Georgia (Shakarian, 2011). Physical armies would fight the Georgians in person while armies of bots hosted on infected computers would overload strategic internet resources of the Georgian government. Hackers—directed by the Russian state—sought to ensure Georgia was defeated both with through force and technologically.

At the same time of the growth of this nascent spam industry, a flourishing legitimate online media and tech industry developed in Russia in the 1990s and 2000s, and Russia’s Search Engine Optimization industry became mature and skilled (Sanovich, 2017, p. 9). These two sectors—both harnessing the immense technical prowess and potential of young Russian computer scientists and engineers—would soon meet in service to the Russian state—or at least those who wielded its power. President Medvedev—who both launched the Russian invasion of Georgia and with whom Obama believed he could “reset” relations—desperately wanted to be popular. A insurgent free press on the social media platform LiveJournal—a blog based social media—was savaging the the Kremlin and providing a venue for political discussions and information (Sanovich, 2017). President Medvedev became known as “blogger-in-chief” and used Facebook, Twitter, Youtube and LiveJournal to wage a charm offensive aimed at influencing the Russian public. He failed. Realizing their failure to control social media through charisma, it was under Medvedev that the Kremlin began employing large scale sophisticated marketing techniques and social media bots (Kelly et al., 2012; Sanovich, 2017). If they could not dominate social media with a populist message and a dynamic spokesman—President Medvedev—then they would spam it with the narratives they
wanted the Russian public to see. While China walled off their internet, Russia saw an opportunity to instead manipulate a new space.

As the Kremlin consolidated its power, it could not shake its biggest fear—a color revolution. Color revolutions preoccupied the mind of the Russian military as these revolutions overthrew corrupt regimes throughout the former Soviet Union and Middle East. It was Ukraine’s Orange Revolution that led to the creation of a new vanguard of youth movements that trolled the opposition and pioneered the kind of social media manipulation Russia would become infamous for (Parfitt, 2005; Osborn, 2005; Sanovich, 2017; Walderman, 2007). It was in this context that Russia’s General Gerasimov—a general somewhat unknown to those outside of the Russian military and faced the prospect of more color revolutions—penned the now famous article *The Value of Science is in the Foresight* where he argues that Russia can transform its warfighting using a Russian version of a color revolution (Gerasimov, 2016b). Russia could turn its “science”—here both its cyberwarfare capability and the technology based political manipulation it uses within Russia to manipulate the public through the fractures within the society that lead to polarization, antipathy and, if exacerbated, chaos. Gerasimov sees the genius of color revolution—engineered social upheavals that provide an opportunity for new leadership that may openly court becoming a client state of the revolution’s sponsor.

Although General Gerasimov consistently claims that hybrid warfare is a western invention and something that Russia should learn from, his work and name have become synonymous with it:

Such definitions almost invariably draw on parts of Gerasimov’s article, in
which he does indeed state that the “role of non-military means has grown and in many cases exceeded the power of force of weapons in their effectiveness.” He also points to the important roles of special operations forces and “internal opposition to create a permanently operational front through the entire territory of the enemy state,” and the blurring of the lines between war and peace….Gerasimov’s article is an important source for understanding Russian thinking, particularly the efforts of the Russian leadership to adapt to warfare in the 21st century... (Monaghan, 2016, p. 67)

This thesis recognizes that hybrid warfare is a word that carries with its own ambiguity—much like the warfare it is associated with. Indeed, the term itself has certainly evolved since its original creation in the West (Monaghan, 2016) Nonetheless, there is a growing body of literature around the term and this thesis will use it, because Gerasimov’s approach is so closely associated with it. When this thesis refers to hybrid warfare it is referring to a blend of conventional kinetic operations combined with other non-conventional tactics, such as political meddling, economic shocks and psychological, behavioral and social meddling.

Further, this thesis generally refers to Gerasimov’s “approach” rather than the “Gerasimov Doctrine” because there is no evidence this is a “doctrine” of the Russian military—especially in terms of some sort of dogmatic and complete approach to war (Galeotti, 2018; Galeotti, 2014). Gerasimov’s ideals appear to be evolving based on his experience in the war in Eastern Ukraine, Syria and various operations around the world. Although The Value of Science is in the Foresight is one of the best articulations of Gerasimov’s approach (especially the idea of exploiting social fractures), Gerasimov
tends to refine and update his thoughts in a yearly speech he gives at the Moscow Conference on International Security. Portraying his approach as anything less than adaptive, malleable and continually being refined would be wrong.

Further, Gerasimov’s articles and speeches are part of a larger debate within the Russian government and military as it modernizes from Soviet era technology and approaches. As this thesis will discuss later, Gerasimov’s position and connections inside the government means he is a key participant in this debate. The Russian military has undergone a significant, expensive and large-scale modernization effort, and it is without doubt the tank commander of the brutal Chechen conflict who now serves at the highest echelons of Russian military is trying to convince the military to adapt and improve western approaches to allow Russian to compete as a global hegemon—not a marginalized backbencher. Gerasimov wants to beat the West, not merely match it: “We must not copy foreign experience and chase after leading countries, but we must outstrip them and occupy leading positions ourselves. This is where military science takes on a crucial role (Gerasimov, 2016).” Gerasimov, though, is likely both portraying his own thinking and that of others within the Russian military and government. With every speech by General Gerasimov, we see someone committed to turning what he sees as the Western military color revolution approach back against the West and its allies—including Ukraine—to create a stronger, modern and more effective Russian military.

Research Problem

This thesis’s central research question is: “To what extent is Gerasimov’s ‘hybrid’ warfare approach being used in Russia’s military intervention in Ukraine?” Debate over
exactly what is Russia’s strategy in Ukraine is ongoing, and as the war continues, the debate demands more analysis and scholarship.

Research Proposition

I hypothesize that, in large part, Gerasimov’s hybrid warfare approach is essentially how the war in Ukraine is being conducted—with the annexation of Crimea being an almost flawless execution of it and Eastern Ukraine being a much less successful implementation that has largely failed—for the time being. The Russian military has thus resorted to sending thousands of conventional and special operations forces to fight the Ukrainian Military instead of a robust local separatist movement. This thesis also posits that General Gerasimov’s approach is firmly embedded within the evolutionary track of the Russian military where information and cyberwarfare campaign are being used in concert with conventional and Special Operations forces.
Chapter II.

Gerasimov’s Information War

This section argues that Russian concerns over a domestic color revolution combined with an unscrupulous private sector, incomplete democratization and an ambitious Russian military sector led to the creation of the modern misinformation machine that is being aimed at Ukraine. Gerasimov’s approach relies heavily on the effectiveness of the technology behind its social manipulation, and it is incorrect to simply dismiss it as a reformulation of past Soviet disinformation and deception methods.

As the 1980s were coming to a close, a new reality seemed to be emerging. Oil prices, which had long acted as an international subsidy for communist and socialist regimes around the world, fell from their heights in the 1970s (Holodny, 2016; Ermolaev, 2017). Gorbachev was trying to transform the Soviet Union—which had slaughtered millions through wars, starvation and purges—into something new and western sounding—perestroika and glasnost, which roughly mean restructuring and transparency. Chinese nationalists sent shockwaves around the world as the occupied Tiananmen Square—a symbol of the Chinese nation—and demanded greater political freedom. It seemed the long march for the freedoms and ideas first dreamed of in the Enlightenment and fought for in countless battles and proclaimed in a thousand marches were finally winning in the world. Freedom was winning.

By December 25, 1991, a weary Gorbachev—who had spent the night before weeping at his failure—called George H.W. Bush to wish him a Merry Christmas (O’Clery, 2016). Borrowing a pen from the President of CNN, he signed the Soviet Union out of existence (Oberdorfer, 1992; O’Clery, 2016). From an office arranged for the
occasion, he delivered a final address as Yeltsin’s men moved his belongings out of the
official residence where he had lived as the leader of one of the most powerful and feared
empires in world history:

The process of renovating the country and radical changes in the world
turned out to be far more complicated than could be expected. However,
what has been done ought to be given its due. This society acquired
freedom, liberated itself politically and spiritually, and this is the foremost
achievement which we have not yet understood completely, because we
have not learned to use freedom. (Gorbachev, 1999)

The news conference had been attended mostly by American journalists—the Russian
media had lost interest (O’Clery, 2016). And so, the last Premier of the Soviet Union
became a mere citizen of the new Russian Federation. The Nobel peace prize winning
USSR leader Gorbachev who had dominated the world for half a decade became nothing
in an instant as Lenin and Marx’s cruel experiment ended in Eastern Europe. The
President of CNN asked for his pen back (O’Clery, 2016).

A new experiment was beginning, though. Could the principles of democracy that
had worked so well in Westernized countries and Japan since World War II transform the
former Soviet Union into prosperous and free countries as well? Or would it return to
authoritarianism?

Although the majority of nations around the world were a democracy or moving
in that direction by granting political freedom, it is the ancient Greeks that could have
best answered this question for the new Russia rising from the ashes of communism and
authoritarianism. Athens is often pointed to as the father of all democracies, but it was the
tortured parent of modernity. It succumbed to coups by the oligarchic class—including a puppet regime controlled by Sparta that conducted brutal political pogroms that left over a thousand Athenians dead, and when democracy was finally restored, a jury of several hundred voters delivered a guilty verdict against their greatest citizen—Socrates—and sentenced him to death (Crain, 2016; Martin, 2000). In the Republic Plato (1992) would suggest philosopher kings as a solution to Athen’s failed democracy because they could exercise a strict control over those who stir up the passions and praise the unvirtuos and tyranny.

Russia had no virtuos philosopher kings. It had Yeltsin. Yeltsin likened himself to Russia’s George Washington—a hero of his (Ostrow et al., 2013). The rose-faced drunkard was no George Washington. Yeltsin and his allies sold off Russian state assets for a pittance—finishing a process of economic consolidation by oligarchs that began under Gorbachev’s economic reforms and efforts at a partially free market (Reddaway & Glinski, 2001). A similar process began under Ukraine’s first President Leonid Kravchuk who helped elevate the oligarch to be Viktor Medvedchuk (a russophile whose later daughter would have Putin as a godfather) to prominence and facilitated the corrupt privatization of the former Soviet assets (Wilson, 2015, p. 270; Bazaluk, 2016). Kuchma relied on eastern Ukraine-based oligarchs—such as the Dnipropetrovsk based oligarchs (Matuszak, 2012). This included one of the eventual leaders of the Orange Revolution—Yulia Tymoshenko. Indeed, virtually every party in Ukraine since the fall of the Soviet Union has been backed by one of a handful of Oligarchs—although in the last Presidential election it was an oligarch himself (Petro Poroshenko) who was the candidate and victor (Åslund, 2015).
These part criminal, part businessmen oligarchs had just as much influence in Russia. Yeltsin’s seven bankers—the oligarchs whom he allied himself with and enriched him—funded the controversial President’s campaign and enriched themselves through their connection to him (Johnson, 2000). Much like Ukraine, the favored Oligarchs changed with each new president. For Yeltsin, the corruption that had helped him retain his grip on power and enrich himself and his family would be the death nail for his presidency. A Swiss firm was reported to have bribed Yeltsin and other members of the Russian government with millions of dollars in kickbacks for lucrative renovation contracts to restore the Kremlin (LaFraniere, 1999). Although the head of the Federal Security Service of the Russian Federation (FSB)—a Yeltsin loyalist—was able to force the resignation of Russia’s chief investigative prosecutor by filming him having sex with several prostitutes in a honeypot scheme, the pressure on Russia’s embattled and iconic demagogue was too much. Renewed terrorist attacks by Chechen Rebels after the humiliating defeats of the Russian military during the first Chechen war and the controversial Khasav-Yurt Accord that gave Chechnya de-facto autonomy were cutting deeply into his public image (Schaefer, 2010). Further, impeachment proceedings against the president instigated by the communists and, more generally, the Duma’s many attempts to undermine him were pushing the president’s approval into single digits (Nelson & Kuzes, 1994). The corruption scandal made the president realize he needed a successor who was not his political opponent and would pardon him of all his crimes. His choice was Vladimir Putin who had already helped get the government’s chief prosecutor fired through the honeypot scheme mentioned above; through this Yeltsin avoided prosecution for his own corruption in office and his family and those around him (Ioffe, 2017a).
The man who had studied George Washington and often proved to be his own worst enemy did not allow his own resignation to follow the same chaotic pattern as that of Gorbachev. Instead, he delivered a powerful, introspective and paternalistic televised speech that echoed the fears of Gorbachev and was remorseful at his own inability to move Russia to the successful democracy it had expected:

I want to ask you for forgiveness, because many of our hopes have not come true, because what we thought would be easy turned out to be painfully difficult.

I ask [you] to forgive me for not fulfilling some hopes of those people who believed that we would be able to jump from the grey, stagnating, totalitarian past into a bright, rich and civilized future in one go.

I myself believed in this. But it could not be done in one fell swoop. In some respects I was too naive. Some of the problems were too complex. We struggled on through mistakes and failures. At this complex time many people experienced upheavals in their lives. But I want you to know that I never said this would be easy....

I am leaving. I have done everything I could. (Yeltsin, 1999)

He had given Russia the only gift he could still give—a peaceful and stable transition from his failing presidency. Later that day Putin gave him a full pardon and a lifetime pension (Bohlen, 2000). Democracy and liberalism were harder to engender in Russia than Yeltsin and his western partners had believed. In fact, they were harder for Yeltsin himself to embrace fully in his presidency than he had believed.
Putin would lay out the central thesis of his Presidency the day following Yeltsin’s dramatic surrender of power—stability. He promised the Russian people:

I am drawing your attention to the fact that there will be no power vacuum, even for a moment…[t]here has been no vacuum, nor will there be one. I want to warn that any attempt to exceed the limits of the law, and Russia's Constitution, will be decisively crushed. (Bohlen, 2000)

There would be no resurgence of communism. There would be no coup. No chart illustrates Putin’s steady hand promise fulfilled than the steady value of the Ruble following his ascendancy to the presidency until the war in Ukraine (Fig. 1). Currency within the post-Soviet republics periodically engaged in financial market whiplash, but Putin, whether through skill or by presiding over a relatively long period of high oil prices with a petro backed ruble, has presided over a remarkably stable Ruble for most of his reign.
Putin was able to use his relative success compared to Yeltsin to consolidate his control over the country, rollback democratic institutions and continue the process Yeltsin had begun in terms of solidifying oligarchic control over the economy and politics—although he would make himself the oligarch of oligarchs and the state would serve his political and economic interests (Goldman, 2004). Although Putin found himself catapulted into the presidency by Yeltsin, he later—when firmly in power—would make clear that he did not agree with Yeltsin’s role in the breakup of the Soviet Union:

First and foremost it is worth acknowledging that the demise of the Soviet Union was the greatest geopolitical catastrophe of the century…[a]s for the Russian people, it became a genuine tragedy. Tens of millions of our
fellow citizens and countrymen found themselves beyond the fringes of Russian territory. The epidemic of collapse has spilled over to Russia itself. (Associated Press, 2005)

Indeed, Putin would echo two of the charges leveled against Yeltsin by the communist party during the botched impeachment trial that helped Putin rise to power. They charged, “Yeltsin had illegally broken up the Soviet Union in December” and “had carried out acts leading to the genocide of the Russian people” (Satter, 2003, p. 57-58). This mentality—remiss for the former power and prestige of the Soviets—wedded to hunger for gaining and retaining power in an oligarchy would prove a crucial catalyst for the development of the information weapons that Russia would use in its war in Ukraine.

The war in Ukraine shares similarities to many of the conflicts in the post-Soviet space; the USSR and Russian Empires infused structural tensions into the regions it governed—often inflaming tensions through internal propaganda that set one group against another. Indeed, before the USSR had formally ended and Gorbachev had resigned, the restive republics were already experiencing turmoil. In the eastern and most industrial part of Moldova, rebels were already trying to declare independence before the small Soviet republic declared independence itself (Czerewacz-Filipowicz and Konopelko, 2017, p. 279). This was not eastern Ukraine circa 2014—which had never had serious attempts at secession before Russian interference after the Euromaidan revolution. This was the highly industrialized region of Transnistria, which accounted for much of the GDP of Moldova at the time of the collapse of the USSR and still generates significant output based on those aging Soviet factories (Całus, 2013). The region holds a large strategic stockpile of Soviet weapons—still the largest in Europe—and a large population of eastern Slavs (primarily Russians and Ukrainians) who were the majority
and had ruled the area. During a short and brutal civil war, Transnistrian rebels, with the support of the former Soviet (now Russian) military stationed there, were able to defeat the Moldovan government’s efforts to regain the territory within its internationally recognized borders. The Russian government—although unwilling to recognize Transnistria as an independent country or annex it outright—remains the lifeline for this breakaway republic of Soviet émigrés and continues to keep its military on its territory.

Although many Moldovans avoid this area and it has gone from the most productive area of the country to a decaying backwater that many travelers avoid and the government isolates, its legacy haunts Europe (Bugajski, 2004). Its weapon stockpiles were used during the civil wars and genocides as Yugoslavia collapsed, and it continues to retard the development of Moldova—a country that looks to Romania and the EU for its future economic development. More importantly Transnistria would set a familiar script that virtually every post-Soviet Russian supported separatist conflict has had: (1) a “persecuted” minority (generally ethnic Russians) who identify with the Soviet Union and Russia, (2) a contingent of Russian “volunteers” with Russian military support—especially Russian “Cossacks,” and, (3) propaganda that exploits “fractures” created by Soviet colonization, propaganda and deportation.

Although the Transnistrian civil war was before the reemergence of a strong Russian propaganda media presence through outlets such as RT or Sputnik or the state sponsored spam of recent vintage, the conflict relied heavily on a field made fertile by years of Romanian-phobia engender by the Soviets to counter the fascist Romanian government of World War II (Nantoi, 2013). Indeed, the Soviets continued to fight World War II long after the last bullets were fired by labeling those who opposed them as fascist vestiges—something aided by the fact that fascist Romania and some Ukrainian
nationalists participated willingly in the holocaust and the brutal German rule that called for it (Zabarko, 2005; Ancel, 2017). A decade and a half after the end of the civil war, the Economist found evidence that Russia was using propaganda to try and promote Transnistrian independence through fake think tanks and obscure media outlets (The Economist, 2006). They also noted that the source appeared to be the same one that had earlier tried to discredit Georgian President Mikhail Saakashvili. Indeed, Russia at the same time was training its weapons of information warfare on Georgia to keep it within its orbit and promote the Russophile separatism within it (Ostrovsky, 2017).

Georgia—much like Moldova—has two breakaway regions with Russophile ethnicities—the Abkhazians and Ossetians (George, 2009). These Iranian and Turkic influenced ethnicities were suppressed and Russified during the Russian and Soviet empires and yet retained a disdain for the Georgian majority that they lived among (Human Rights Watch, 2009). During their separatist wars at the breakup of the Soviet Union, they engaged in a systematic and thorough ethnic cleansing of Georgians. The defeat and expulsion of ethnic Georgians from their homes was a bitter pill and humiliation for the new Georgian government. With the election of President Mikhail Saakashvili, a reformist wave pushed Georgia away from the east and Russia and towards the EU and NATO (Stefes, 2006). To gain membership in both, though, the country needed to settle its frozen conflicts. Unfortunately, to end the bloody conflict with the separatist regions, earlier Georgian governments had made a Faustian bargain in a series of agreements made in Sochi that allowed Russian peacekeepers to stay in the Georgian breakaway regions in exchange for peace (Library of Congress, 2015). Georgia—in exchange for peace—had unwittingly surrendered huge amounts of sovereignty for the foreseeable future. Thus, when Saakashvili tried to regain these separatist regions, he
found himself fighting the Russian peacekeepers and, more importantly, the Russian military elements that had illegally entered the territory. Georgia was defeated in less than a week, and Russia recognized the territories as sovereign countries (McNamara, 2008).

Although the Russian military’s involvement was more open, they were able to use the artifice of peacekeeping—given their already legitimized presence in Georgia through the peace deal they brokered. Further, they were able to claim—although the Russian military outnumbered the separatist fighters themselves—that they were supporting their fight and that many who fought in the conflict were volunteers—often North Ossetians in Russia (Human Rights Watch, 2009). Although Soviet propaganda had not provided a solid base for the separatism like in Transnistria, Russian propaganda was carefully crafted from the moment the Russian soldiers began their invasion. Russian journalists—embedded with the military—were able to see carefully scripted “liberations” of ethnic Russians (Lowe, 2008). President Medvedev would accuse the Georgians of committing genocide through actions where “civilians were torched, sawed to pieces and rolled over by tanks” (Radyuhin, 2016). Putin would claim that Americans were aiding Georgian military attacks on the separatist regions—something Russian propaganda would echo through pseudo experts and conspiracy theorists. At the same time, the Russian government tried to actively suppress anything that contradicted their narrative of liberator and defender of the persecuted minorities—including firing an RT reporter who wanted to report on Russian bombing inside Georgia outside the separatist regions (Kirchick, 2014).

More classic techniques—such as delivering realistic fake documents to Western media looking for a scoop—were used to manipulate publications like Der Spiegel, but
Russia had yet to see the benefit in utilizing social media to spread propaganda (Herpen, 2014). In fact, as the Russian government continued its information war against Georgia long after the guns were silenced, its first efforts to counter social media narratives were to shut them down. Their most famous attempt was to silence blogger Georgy Jakhaia—a survivor of the Sukhumi massacre by military units supporting the Abkhaz separatists (Reuters, 2009). No doubt driven by the hellish memory of children being executed and people being disemboweled while alive in his home town with the support of the Russian government, the Georgian professor critiqued the Russian invasion of 2008 to his large social media audience. In order to silence him, Russian linked hackers launched denial of services attack against LiveJournal, Twitter and Facebook—briefly taking down the young platforms (Reuters, 2009). This clumsy attempt at silencing their critic backfired and grew Jakhaia’s following and influence online, but this was the modus operandi for the Russian’s approach to cyberwarfare at the time—having earlier launched denial of service attacks during their invasion of Georgia and in Estonia in retaliation for moving the Soviet Soldier memorial (Harvey, 2009).

By 2010, the Russian government control of traditional media was nearly complete—with the Putin regime controlling directly or through its proxies nearly every newspaper or television station except for a small contingent of marginalized independent media, but the social media sphere—or at least the social media and blogging platform most popular at the time—were thought to be relatively free of government interference (Etling et al., 2010). Internet usage was relatively low at that point compared to now—only 37% of the Russian population—and dominated by urban and more educated users. Rather than use Twitter or Facebook, Russians who used social media—especially for news consumption and political discourse—primarily used a blogging based social media
application known as LiveJournal (Sanovich, 2017). This platform proved a fertile ground for somewhat subversive discussions and campaigns to discuss politics and corruption in Russia. Rather than try to suppress it *de jure*—as China has done with its national control of the internet through monitoring and blocking—the Russian government tried to compete in it initially (Sanovich, 2017). President Medvedev—the Russian President who Obama believed he could reset Russian relations with—attempted to become a social media icon like his US counterpart. Although Medvedev would become known as “blogger-in-chief” for efforts at engaging on Facebook, Twitter, Youtube and LiveJournal, his efforts at projecting influence through personal charisma largely failed and were not followed by Putin when he returned to office for a third term (Sanovich, 2017). Instead, Putin would follow Medvedev’s example in other ways by leveraging Russia’s seedier internet underground of spam, trolling and algorithm manipulation in the private sector.

It is more than a little ironic that Russia’s embrace of capitalism at the urging of the West—albeit a much more oligarchic and extractive form of it—would lead to the development of information manipulation technology that would threaten the very foundations of the West. Within the business world, information manipulation is not uncommon to gain advantage. Amazon has recently fallen under the spotlight for the aggressive trolling by competitors in their marketplace who post false negative reviews for competing products or accuse the competitors of violating intellectual property laws to force Amazon to take down the listing while the claim is investigated (Woollacott, 2017). Similar dynamics are even more prevalent in Ukraine and Russia where seedy companies are paid to troll competitors and promote the company’s own product (Sanovich, 2017). Working often for a pittance, paid trolls and commenters will work
hard to make their target product well respected and the competing products worse. This whole domestic Russian spam industry—helped by the lack of clear Rule of Law—often relies on lies and misinformation to market and trick their targets into using the products or providing them money (Sanovich, 2017). Indeed, selling political lies is not much different morally and technically than trying to sell mysterious and unprovable herbal supplements or falsely reviewing a competitor. The Russians had deep wells of human trolls for their weaponized spam, but they soon realized that if they were going to engage and effectively suppress audience, they would need automated multipliers for their messages:

However, using human trolls for retweeting and reposting is inefficient given that these tasks could easily be automated. Fortunately, by the mid-2000s Russia had a well-established and innovative industry of spam and search optimization. [footnote omitted] Thus originally commercial technology—another child of the flourishing online media and tech industry that developed in Russia without much government interference in the 1990s and 2000s—became a key advantage that the Russian government was able to leverage in its nascent online propaganda strategy. (Sanovich, 2017, p. 9)

Early Twitter bots were much more benign and tasked with generating trivial tweets such as creating poetry in iambic pentameter or sending tweets at certain timed intervals or in response to events (Anderson, 2012).

Before social networking, individuals often envisioned the social robot as something that could engage in human like behavior and trick humans into believing they
were real—perhaps passing the so-called Turing test. In reality, the social robots—as pioneered by marketers and used by the Russian political establishment and government—do something much more profound and powerful en mass: they mimic human social networks that transmit and vet information and have existed in some form back to prehistoric times. This means that they fool both the computer algorithms that are designed to aid these networks to transmit and amplify information—such as in Facebook or Twitter—and the humans who rightfully rely on social cues and collective information processing to understand what is true and false. In this sense, modern times are far worse than science fiction, because they imbue even basic social signals—such as whether there is an emergency—with ambiguity and incredulity.

As social media technology developed and the post-Soviet world became even more restive after all the failed promises of its leaders, the Russian government faced a challenge: how do we control civil society and prevent the kind of revolution that brought us into power? Reborn in the chaos of the failure of communism and noisy and disruptive protests—they knew the power of a revolution and feared one would happen again. By the mid 2000s, Russia knew it could face domestic instability in the guise of a so-called color revolution like the Orange Revolution in their culturally similar neighbor Ukraine that shared many of the same challenges of corruption and mismanagement following the fall of the Soviet Union (Umland, 2012). Indeed, before the 2004-2005 Orange Revolution Kuchma’s mismanagement of the Ukrainian state seemed to follow the “managed democracy” approach of Putin early in his tenure as president (p. 20-21). When the Ukrainian government seemed to break with this distorted version of democracy advocated by Putin and begin to align with western powers while moving away from Russia, Putin moved down a new “special path” of suppressing of democracy,
engendering anti-Western feelings and, most importantly, ensuring that a color revolution would have great difficulty occurring inside Russia (po. 21-22, 30).

It was in this moment—as the Russian elite knew their political hegemony’s days may be numbered—that the social bot birthed the political bot (Woolley, 2016). Before roughly 2010, the social bot was largely the province of the spammer and socially savvy business owner. It was a team at Harvard’s Berkman Center for Internet & Society that discovered some of the first evidence of Russian use of political bots to amplify propaganda coming from Kremlin Twitter feeds and create more effective state sponsored spam (Kelly et al., 2012; Sanovich, 2017). As Sanovich (2017) notes:

The first known large-scale deployment of pro-government bots and trolls in Russia was carried out in support of this engagement strategy of President Medvedev (Barash & Kelly, 2012; Kelly et al., 2012). The troll contingent was, for the most part, recruited by repurposing pro-Kremlin youth movements, which had been created to combat colour revolution on Moscow’s streets and squares (Hale, 2006). Their job primarily focused on...posting diversionary comments in the high-profile opposition blogs (Ananyev & Sobolev, 2017), plus retweeting and reposting pro-government messages. (p. 9)

As Sanovich alludes to, these youth movements are believed to have been started primarily as reactions to Ukraine’s color revolution—especially by international observers at the time (Parfitt, 2005; Osborn, 2005). The group became notorious early on for creating misinformation to discredit the Russian opposition—such as by staging
photos (Waldermann, 2007). In fact, it was Putin strategist and former marketer Vladislav Surkov who created the so-called “nashist” youth movement to counter elements in Russia that could cause a color revolution. Sanovitch believes this internal political demand—to suppress political dissent and thereby guard against a Russian analog to the orange revolution—spurred the “market competition in the Russian tech sector...to efficiently meet this demand and create tools that were later deployed in foreign operation” (Sanovich, 2017, p. 5). Indeed, it is undeniable that these first deployments of computational propaganda were spurred by the internal demands of Russian politics. That being said, Sanovitch’s thesis is incomplete without one key and emphatic proviso: this demand was spurred by an external event, namely the color revolution within Ukraine and the feeling within Russia that it was under siege as the next likely victim of a revolution demanding liberal democracy.

This fear became the preoccupation of the Russian military (especially the General Staff that Gerasimov is Chief of) and General Gerasimov who saw this tool—the ability to spread propaganda throughout social media—as a weapon to be wielded in counter-revolutions against color revolution coups engineered by the West. Gerasimov’s article *The Value of Science is in the Foresight* (2016) is a culmination of this fear and it argues for the use of these sophisticated domestic approaches to be leveraged abroad in future wars where color revolutions are occurring or have occurred. Despite the fact Sanovich and others dismiss Gerasimov’s importance, Gerasimov’s importance is undeniable—as I explain later in a section devoted to this question. Factors such as the General’s formal positions, relationship with Sergei Shoigu, and open and clear advocacy for these hybrid techniques ensure his role in the articulation of Russian military strategy, theory and tactics.
Although Gerasimov published his famous article *The Value of Science Is in the Foresight* in 2013 roughly a year before Euromaidan ended and the government of Ukraine fell, he clearly explained the approach he advocated again at a Security conference at a Radisson hotel in Moscow shortly after Kiev’s 2014 revolution. There General Valery Gerasimov, now Chief of the General Staff of the Armed Forces of the Russian Federation and First Deputy Minister of Defense of the Russian Federation, explained that he wanted to restore geopolitics to a multipolar world with spheres of influence again (Cordesman, 2017). Color revolutions are an “adaptive approach” to war—he mused—where one could fight low cost, destabilizing wars across the world (pp. 12-13). Sergey Lavrov, Russian Minister of Foreign Affairs, was also at the conference in a speech that was paired with Gerasimov’s. He argued the United States was “using the ‘Color Revolution’ to serve their own interests, impose their own values, and end in creating new global tensions” and had isolated itself from Russia (pp. 9-10). The West was trying impose values on other nations that they did not want to adopt.

For Gerasimov, his strategy for hybrid warfare—as it has come to be known—was not particularly innovative. He was simply turning the color revolution method of war into a Russian technique; Russia should wage wars in the same hybrid fashion he saw the west fighting its “wars”—e.g. color revolution coups (Gerasimov, 2016). Gerasimov’s articulation of this principle in this article and eventual implementation in the field led this approach being called the “Gerasimov Doctrine.” In his written work, Gerasimov argues many points in his lecture and writings, but his hybrid war (a word and concept not of Russian origin by later embraced by Russian and Ukrainian military thinkers) has three essential elements. First, Russia should find and leverage “differences” in a society—such as ethnic and cultural tensions—and transform them into
social contradictions and fractures that undermine the social stability (p. 28). From a systems theory standpoint, these are the points of leverage within the system through which you can shape it. Second, protection of human rights and the need to keep the peace will be used as a pretext to intervene militarily after the situation has been deliberately exacerbated. Third, if the West complains about Russia’s action, the country can rebuff them by noting the numerous invasions such as in the Balkans, Middle East and North Africa under the pretext of protecting human rights (such as in Libya) and protection against terrorism (e.g. Iraq and Afghanistan). For Russians—especially the political elite—the US and more broadly the West has relegated Russia to second-tier power status—imposing double standards on Russia that they do abide by themselves. The US and its allies can bomb sovereign nations to protect the rights of a minority—such as the Muslims in the Balkans—but the same nations chafe at Russia protecting the Russian and Russophile minority sprinkled throughout the former USSR territory (Walker, 2014). This argument resonates both at home and abroad—something that can be brought out again and again when the US critiques Russian foreign meddling.

Many papers argue Gerasimov’s influence is overblown—as seen by Sanovitch’s dismissal of his importance. Many claim disinformation, maskirovka and other methods of information warfare have long been used as a tool of subversion by the Soviets and Russians—pointing to Soviet claims that the US had invented AIDS or the many times by which the Red Army used deception to help defeat the Nazis (Grimes, 2017; Taylor, 2016). In many ways, this is an argument that does not understand that Gerasimov’s approach inherently relies on advanced technology to disrupt and destabilize social structures—technologies like Facebook and Twitter that did not exist during the days of the USSR. Indeed, Gerasimov is advocating using cutting edge science and technology as
a method of exploiting these fractures. The fractures themselves, though, are generally of Soviet vintage and not the result of more modern events. In many ways, conflicts in the post-Soviet space are the perfect opportunity to apply the Gerasimov doctrine, because Russia can exploit the fractures it helped create in its empires of the past.

The iron grip of the USSR kept ethnic and cultural rivalries in check—much as it did in Ba’athist Iraq and Tito’s Yugoslavia. Whether it is the Bosniacs, Croats and Serbs of Yugoslavia or the Sunni, Shiites and Kurds of Iraq, internal contradictions can be kept at bay with the chains a strongman or an autocratic oligarchy places on society. The countries within the former Soviet Union are no different, and the tensions that have remerged as the national interests of the ethnicities within these countries collide—often fostered by the Russia Federation as it seeks to regain status as a regional hegemon. Indeed, for Russia, it is easy to exploit the internal contradictions within former countries of the Soviet Union, because they are often due to ethnic Russians living within these countries and the colonial policies of Russia and the USSR that put them there. Indeed, Ukraine—despite the fact a large number of Ukrainians still live within Russia and/or are married to or are related to ethnic Russians—has long struggled with the internal contradictions of large populations of ethnic Russians within Ukraine, having a common cultural ancestor in the Kievan Rus and yet being a separate ethnicity and culture with its own language (Yekelchyk, 2007). Indeed, Ukraine’s longstanding quest for independence has always been at odds with its close relationship with the Russian nation and culture. Whether it is Bandera’s Faustian bargain with the Germans during World War II to free Ukrainians from the Soviets or the Ukrainian communists who ensured Ukraine remained a separate union Republic within the Soviet Union and not merely part of the Russian Soviet Federative Socialist Republic, Ukraine has sometimes awkwardly tried to create
clear lines in the ambiguous landscape of Russian and Ukrainian culture (Solchanyk, 2000; Garrett, 1997).

For Gerasimov, though, this ambiguity and the inherent tensions and contradictions within Ukraine provided easy points of fractures through which to shatter the nation of Ukraine—much as he theorized in 2013. Even though Ukraine (including Crimea) had overwhelmingly voted for independence from the USSR, Crimea remained dominated by its ethnic Russian majority—many of whom were connected to the Russian military that remained on the peninsula (Yekelchyk, 2007). Likewise, in Eastern Ukraine, a substantial minority of ethnic Russians (as well as the Ukrainian majority have lived for generations under the yoke of the Russian Empire) continually thwart the more nationalistic Ukrainians in western Ukraine from rolling back the russification that occurred in the country while western Ukraine was being dominated by western conquerors, such as Poland and the Austro-Hungarian empire (Wilson, 2015; Solchanyk, 2000). Orientalist historians argue (much as they do with respect to the Balkans) that this led Ukraine to develop two parallel Ukrainian civilizations—one that embraced the values and culture of the Renaissance and one which remained locked in the medieval know-nothing mentality of the peasantry and oligarchs (Yekelchyk, 2007; Wilson, 2015). For Gerasimov, Kharkiv, Dnipro and Yanukovich’s hometown of Donetsk are culturally closer to Russia than Ukraine despite being within Ukraine—easily acquired from a shattered Ukrainian state. Gerasimov, though, quickly found that eastern Ukraine and Crimea were very different regions—as were the somewhat Russophile regions like Odessa.

Although there is evidence Russia has sought to destabilize the Odessa region, the efforts appear to have largely failed (Korewa, 2016). Russian efforts have instead
concentrated on Crimea and eastern Ukraine as centers of the hybrid war against Ukraine. As noted above, Crimea is the only region of Ukraine with a majority of ethnic Russians—many of whom are Russian nationals who simply live in Crimea as a consequence of Russia’s military presence there (Goble, 2015). The peninsula has a heavy ethnic Russian presence along the coast while much of the interior remains a mix of Tartars and Ukrainians. The peninsula, unlike the Donbas, received an autonomous status within Ukraine upon the country’s independence and has had separatist agitation from a minority of the Russian majority since the creation of the Ukrainian state—although right before the annexation separatism was relatively unpopular (Menon & Rumer, 2015). Many of these separatists point to Kruschev’s “gift” of Crimea to the USSR Ukrainian proto-state as a foolish move—given that the peninsula’s connection with Russia since the late 18th century and its large ethnically Russian population (Keating, 2014). A counter argument is that an ethnic Russian majority only occurred after World War II and the deportation of the Crimean Tartars by Stalin (Kramer, 2014).

Eastern Ukraine, on the other hand, was never a “gift” to the proto-Ukrainian state. It contains cities such as Kharkiv and Dnipro that are core to the Ukrainian culture and national identity—although the region was depopulated by war and starvation engineered by the Soviets and Nazis (Yekelchyk, 2007). These slaughtered Ukrainians were often replaced with ethnic Russians who came to the region to participate in its rising Soviet industrial machine (Nalyvayko & Bulanenko, 2016). Russian propaganda argues that the area is simply the Russian empire’s almost mythical Novorussiya—a colonization effort by the German born Russian Czar Catherine the Great, but despite the fact area has a Russian-speaking Ukrainian majority and a relatively large ethnic Russian population, large populations of Ukrainians also live beyond the Ukrainian border within
the borders of Russia—land not claimed by Ukraine but traditionally inhabited by ethnic Ukrainians (Kulchytsky, 1945). Indeed, the Ukrainian borders have never been a strained view of the outlines of the regions in which ethnic Ukrainians live—they are a very conservative version. The fact that Russians attempt to expropriate the Ukrainian cultural heritage, such as the Cossacks or even the Kievan Rus from which Russian gets its name, does not transform Ukrainian culture into a Russian sub-genre—it is Russian culture that is the true derivative.

Thus, in Eastern Ukraine, the Russians did not run into a Ukrainian periphery—territory that could easily be placed inside Russia’s own borders—he was planning for an invasion of the core of Ukraine. Despite the east’s poor judgment in elections and affinity for Russia, it was there, near cities such as Dnipro, that the ancient Cossacks hosts lived and Ukrainians forged some of the early outlines of the modern Ukrainian state (Wilson, 2015). Thus, the differences within the inhabitants of eastern Ukraine between—which range from those who are firebrand Ukrainian nationalists to those who yearn for closer ties with the Russian state—are fundamentally different from Crimea where many are simply Russians (many times with Russian citizenship) who have chosen to stay in Crimea and want their home country to control it (Toal, 2017). Historians in the orientalist tradition tend opine on the fundamental difference between the regions of Ukraine that were under Russian subjugation for centuries and those subjugated by powers to the west of Ukraine—much as they do when speaking about the Balkans. As noted above, though, in practice this simply meant parallel developments of the Ukrainian identity in both eastern and western—and the diaspora (Kappeler et al., 2003; Wilson, 2015). This division did not make them any less Ukrainian—much as the Kurds of Turkey, Iraq, Iran and Syria remain Kurdish. Indeed, Ukrainians may be of different
political and ideological colors but they remain part of the same fabric of Ukrainian identity—something the Russian government did not properly envision. Ukrainians—despite their homeland being divided among nations and many living abroad—have stubbornly clung to their ethnic identity even in the face of persecution and disparagement (Kappeler et al., 2003; Yekelchyk, 2007).

Polls both before and after the invasion confirm that Eastern Ukrainians—despite their differences with Western Ukrainians—remained committed to remaining in Ukraine—although most Eastern Ukrainians disagree with the use of violence to settle the conflict (Swab, 2014; Popeski, 2014; Poushter, 2015). This is a sign that the information warfare Gerasimov argues for has failed in many respects. The main difference remains the degree to which the two regions believe Ukraine should align with Moscow—although the aggression against Ukraine has driven many Ukrainians from wanting to be closer to Russia to serving in volunteer battalions fighting against it (Popeski, 2014; Cohen & Green, 2016). In fact, it was volunteer battalions financed by oligarch Ihor Kolomoyskyi that helped prevent the expansion of the separatist movement into Dnipropetrovsk (Pinkham, 2015; Cohen & Green, 2016). Ironically, the Ukrainian state has actually been strengthened in some ways by the war in the east and the Crimean annexation—as seen by a poll demonstrating greater support for an independent Ukraine a year into the conflict (Synovitz, 2015). Controversially, some scholars and Ukrainian elites argue Ukraine is actually better off without the Russophile east—a region that has caused one headache after another for the Ukrainian state from spawning hyperinflation to pay miners to voting in corrupt and incompetent Russophile officials into office—like Yanukovych (Motyl, 2016). Regardless of the position of the Ukrainian public and elites, the longer the east remains occupied and estranged from Kiev the more reliant it becomes
on Moscow. Although reintegrating Eastern Ukraine into Ukraine may reintroduce some of the same poison that has inhibited the Ukrainian state before the war, surrendering it to Russia would only grant Russia a surprising victory and embolden the Russian military into spreading Gerasimov’s hybrid warfare deeper into Ukraine—including Kharkiv or Kiev where plentiful russophile Ukrainians and ethnic Russians represent a base for a coup attempt (although Kharkiv has a much stronger russophile base) (MacKinnon, 2014).

In many ways, Crimea was the lowest hanging fruit because of the large number of Russian nationals who lived there, and Crimea’s differences were exacerbated by the Euromaidan revolution’s patriotic fervor. These Russians needed very little encouragement to support Crimea’s annexation. Many Russian nationals had only begrudgingly sought Ukrainian citizenship upon the fall of the USSR—making many Crimeans simply Russians who lived in Ukrainian territory (Knott, 2015). Angry at the ouster of a president they had overwhelmingly voted for and the Western direction of the new Ukrainian revolutionary government, the possibility to exploit the growing contradictions and fissures between Russian Crimeans and the Ukrainian state proved to be a perfect opportunity for the Russian to apply the hybrid warfare technique Gerasimov describes; indeed, Yanukovych had escaped by way of Crimea through the efforts of sympathetic Crimeans and the Russian military (Kravchenko, 2014). As Euromaidan spread across the country and toppled one corrupt local government after another, Crimea had remained firmly in the hands of the corrupt establishment. Although there was a fringe party that argued for annexation by Russia in the election preceding Euromaidan, they were soundly beaten by Yanukovych’s Party of Regions (Carbonnel, 2014; Menon and Rumer, 2015). Either because of indifference, cynicism or apathy, the population of
Crimea had long since accepted being a part of Ukraine, and yearly embraced the throngs of tourists from other parts of Ukraine who came there. Even if the Crimean residents had been intent on independence from Ukraine, they had neither the resources nor the power to overcome the Ukrainian government forces there. Under Gerasimov’s approach, though, this was not an issue. Russia—as Gerasimov outlined in his 2013 paper and speech a year earlier—believed it could tip the balance in Crimea in their favor through an adept use of clandestine special forces paired with political and information warfare that would exacerbate social fissures to become breaks.

The tactics to accomplish this follow Figure 2—although Crimea was won too quickly to really follow closely the scheme Gerasimov envisioned Western powers as using. The main tactics were several. First, Moscow already had the coalitions within Crimea it needed by virtue of its large military presence and the many Russian nationals and these provided the patina of a local moment (Markov et al., 2016). In fact, the political opposition in Crimea to the Euromaidan movement was Russophile by its nature since it was composed primarily of the ethnic Russians and Russian nationals who dominated Crimea. Second, Russia and Ukraine were heavily dependent on each other in economic terms at the time, and Russia could exert heavy political and diplomatic pressure that Ukraine could not match. A well-placed threat to cut off the gas during winter or the placing of a ban on certain Ukrainian goods could strike a heavy blow to the Ukrainian economy and people—especially right after the revolution toppled Yanukovych. Because Euromaidan occurred in the dead of winter, Russia’s perennial gas blackmail was one of the most obvious tools for the Russian government at the time. Third, although this early Gerasimov chart is unclear as to when an influence and propaganda campaign should start, Russia had been engaging in an information war against Euromaidan before the
Crimean operation began or Yanukovych fled to Russia (Darczewska, 2014). Whether it was linking the movement to fascism, claiming it was simply a lawless riot or calling it a “coup” upon its success, Russian propaganda was a nonstop “firehose of falsehood” attack on the new Ukrainian government and the movement that created it (Paul & Matthews, 2016).
Fourth, Gerasimov understood that the threat of military action was a weapon in and of itself. Russia openly shuffled and massed its troops all along the Ukrainian border as though ready to engage in a large a full-scale invasion as the Moscow backed regime fell and afterward—especially in the run up to the Crimean referendum (Myers & Smale, 2014). Further, it conducted military exercises to intimidate the Ukrainian government and show military capability—something it regularly does now on the Crimean Peninsula (Alpert & Solomon, 2014). By and large—even after the invasion of the east—these border massed forces have generally been spectators and a show of force—not the special operations forces (SOF) vanguard that has been conducting many of the military operations in Ukraine (Bukkvoll, 2016).

Gerasimov’s fifth tool is the use of SOF and mercenaries—or private military companies as Gerasimov refers to them. In many ways, this is the heart of Gerasimov’s approach. Although SOF units often embed themselves within foreign fighting units, Russia took this to another level by tearing off any insignia that linked Russian SOF to Russia and then pretending they were locals—an easy task given the heavy Russian national presence (MacAskill, 2014). Even so, the fact that they were Russians was barely concealed. Indeed, perhaps at no other time in history was the invasion of another country so covertly brazen as during the attack of the “little green men” of Crimea (Stallard, 2015).
The effectiveness of Gerasimov’s approach is clearly shown through its extremely effective implementation in Crimea. The invasion of Crimea proved to be both an agonizingly slow and terrifyingly fast humiliation of the young Ukrainian nation as the Russians pantomimed local opposition and slowly took over one Ukrainian military base and government facility after another with tense stand-offs but little violence (Herszenhorn & MacFarquhar, 2014). Many Crimeans who served in the Ukrainian military defected (Withnall, 2014). Local Crimeans were faced with the difficult decision to support a government led by people they neither voted for nor respected or allow Russian special forces and their mercenaries to essentially shove the Ukrainian authorities out as Kiev’s democrats reeled. The government from Euromaidan—less than a month old—held only a tenuous grip on power without a new election to provide them legitimacy, and they understood direct war with Russia could shatter the country into the pieces Gerasimov and the Russian government wanted so desperately it to break into. Sadly, the previous governments of Ukraine and Crimea governed with extreme corruption and mismanagement that had left the region discontented with Ukrainian rule (Greene & Migaki, 2014). While most Crimeans passively stood and accepted Russia’s invasion—whether they supported it or not—the Tatars who had remained after the mass deportations from the Stalin era opposed it (Vasilyeva, 2016). Many Crimean leaders—upon leaving to lobby the international community to stop Russia—were barred from their homeland while others simply disappeared much like they would have in the Soviet days (Cole, 2017; Blair, 2016). Gerasimov’s war in Crimea was complete.

The deportations of Stalin and the colonization of Crimea during the Russian empire and the USSR laid the preconditions of a population more connected to Russia than Ukraine—the country with which Crimea is geographically connected. Indeed, you
could argue that many of these colonial Crimeans are more connected to Russia than even Crimea—looking to Moscow more than Simferopol, Sevastopol or Ukraine’s capital Kiev (Rosenberg, 2017). It was this fissure that Gerasimov exploited with breathless ease as he waged his virtually bloodless counterrevolution in Crimea. He exploited the “differences” between the Russian nationals, ethnic Russians and ethic Ukrainian and then transformed them into contradictions and fractures that ultimately lead to the annexation of Crimea and the peeling away of the peninsula from the Ukrainian State for the foreseeable future.

As noted above, allegations of human rights abuses are a key propaganda tool in Russia’s information warfare toolkit. Russia has unleashed a firehose of propaganda claiming mass human rights abuses by the Kiev government as well as through its foreign ministry’s so-called “white book”—a fictionalized narrative of supposed human rights abuses by the Ukrainian government that attempts to use Western human rights language and norms as weapons to discredit Ukraine (RT, 2015b; Denber, 2014). Needless to say, this effort to paint Ukraine as a savage human rights violator of ethnic Russians while Russia backs rebels who cite Stalin while executing citizens for alleged theft has failed; Russia has not helped this perception by supporting a regime in the middle east that uses chemical weapons on children and civilians—going so far as to blocking UN condemnation of these attacks (Office of the United Nations High Commissioner for Human Rights, 2014; Roth, 2017). Because of this failure, Russia has never been able to admit to its military presence in Ukraine and then justify it as a measure to prevent human rights abuses of ethnic Russians. Unlike the Balkans where war is common among the competing ethnicities, most Ukrainians would have laughed off even the idea of a war with ethnic Russians as absurd before Russia created the conflict in the east. The Russian
government may, though, be playing a long game—knowing that virtually every military has moments of rogue soldiers and poor decisions where soldiers violate human rights. At that point, the Russian military presence in Ukraine may be then acknowledged as the soldiers transform and drop their performance as local rebels and become “peacekeepers.” At this point, Russia has been unable produce a narrative that would support a Russian “peacekeeping” operation—considering it is virtually undisputed internationally among world leaders that Russia is the instigator of the war within Ukraine. Despite the fact that Gerasimov’s vision for hybrid warfare is unfulfilled in Eastern Ukraine, in Crimea the operation was so successful the military did not even have to pose as peacekeepers—it was to able grab the territory posing as locals with only minor skirmishes.

If Gerasimov’s articulated vision is fulfilled in Eastern Ukraine and Russia deploys as guardians of human rights and peacekeepers, the Russian state will defensively engage in an information warfare attack that lambastes the West for its hypocrisy due to its many interventions to justify it. One of Russia’s favorite examples of the US invading based on a pretext—and an example General Gerasimov uses—is its intervention in the war in Yugoslavia—something that led in the end to the recognition of Kosovo as an independent and sovereign state (Cordesman, 2017). Many Russian elites believe Russia is a Slavic hegemon with a duty to intervene, protect and (as far as possible) rule the Slavic world—including the Serbians (Gvosdev & Marsh, 2014). For Russia’s elite when the West fought against the Serbs, it was unforgivable. When the West attempted to integrate it’s most important former province (Ukraine) through what they view as a western engineered color revolution, that was even more unacceptable. To the Russian establishment the disembowelment of the Ukrainian state project through the
pretext of the protection of the ethnic Russians who choose to live there is no stretch—it is a contorted version of the logic the West used when protecting the Albanians of Kosovo against the Serbs who sought to drive the Albanians out of what they viewed as Serbian ancestral lands. Ukrainian nationalists trying to restore the primacy of the Ukrainian language and culture in the Russophile areas of Ukraine is the same to the Russian leadership; if the West can stop the Serbs from driving Muslims from an ancestral homeland stolen by the Ottomens, why can the Russians not repel Ukrainians trying to drive out Russian Soviet colonists? The difficulty is that there is no evidence that ethnic Russians within the east would have fought the Ukrainians without Russian support.

Even if this argument does not hold up, Gerasimov can argue using the US interventions in the Middle East and central Asia that it is completely justified in its intervention in Ukraine on the grounds its security is in danger (Cordesman, 2017; Gerasimov, 2016). Indeed, the US invaded Iraq and Afghanistan under the guise of protecting its own security. In Iraq, those arguments proved to be based on incorrect intelligence. In this case, Ukraine is actively trying to join an organization that was created to oppose Russia when it was part of the Soviet Union (and ironically Ukraine was as well). Of course the cold war is over, so the security threat is more imagined than actual. Even so, this cold war thinking still exists in many Russians—even if leaders such as Putin are more afraid of losing power to a democratic revolution than of an invasion.

In sum, the political developments in Russia led to a weak and underdeveloped democracy where information manipulation was key. Although the Russian government initially failed in its efforts to engage with or suppress social media, its use of sophisticated state sponsored weaponized spam has made it a formidable actor in the
information domain. Its development of aggressive social media propaganda techniques appear to be a direct response to the Orange Revolution and the creation of counterrevolution movements. Gerasimov’s approach does not merely envision information warfare as the sole use of the cyber domain—it envision using full scale cyber attacks that weaponize viruses and malware. Fortunately for Gerasimov, Russian capability in this area is already extremely high and already play an important role in Russian military engagements.
With the advent of every new age, warfare advances and increases its deadly force. Iron defeats bronze. Steel defeats iron. Bayonets become mere symbols against the power of the machine gun. Today, we are in the era of war via computers. With this comes a whole host of new questions. What is an act of war? Indeed, what is war? The Pentagon has announced that cyber attacks can be considered acts of war (Gorman & Barnes, 2011). Gerasimov appears to view cyberwarfare as one of the domains of war himself and part of what an increasingly aggressive NATO will use as a pretext for war—despite the fact tracing sophisticated attacks can be quite difficult (Fig. 3; Gerasimov, 2016a). In fact, the Pentagon released its “cyber strategy” for the first time in 2011 to herald in this new age (Epatko, 2011). If you bring a country to its knees by disabling its infrastructure, would a lethal counterstrike be justified? Cyber weapons such as Stuxnet and Flame have astounded computer scientists and engineers in their complexity and effectiveness (Nachenberg, 2012). Russian cyberwarfare is at the cutting edge and represents a key part of Gerasimov’s vision of a Russian military that wages these lightweight, hybrid conflicts in the mold of the color revolutions.
Cyberwarfare and hacking are relatively young because computers have increased in sophistication exponentially. Roughly four years after the end of World War II, the computer virus was born in the mind of John von Neumann—a Jewish Hungarian immigrant who worked on the Manhattan project (MacRae, 1992, pp. 37-38, 67-68; Szor, 2005, Chapter 1, Section 1.1). Von Neuman was also one of the chief architects of the modern computer by introducing the concept of memory for information storage and binary operations (Szor, 2005, Chapter 1, Section 1.1). It was during World War II that computers began to show their incredible power for good and evil. On the one hand, IBM’s punch card run computers (often housed within the concentration camps) helped to catalog the millions of Jews marked for extermination (Black, 2011, pp. 20-21). On the other hand, the brilliant Alan Turing (the creator of the eponymous Turing Machine) would create an electromechanical computer “bombe” that would crack the enigma.
cipher of the Nazis by emulating its structure and reversing the cipher process in a way no single human could (Page, 2009, p. 145). The ability to perform repetitive and complex calculations has been sought after by humans for thousands of years. Some claim the first computer was built two-thousand years ago by the Greeks, who created a device to calculate planetary motion and the timing of the Olympics (Sorrel, 2008). It was Charles Babbage, though, who in the nineteenth century was inspired by the punch cards of the loom machine to create an “analytical engine” that could perform highly complex mathematical operations, such as multiplication, by taking in cards with information (Babbage, 2002, pp. 88-89; Rao, 1994, pp. 2-3). Even though he would die before he was able to create the machine, his ideas fundamentally shaped computer architecture and led to the creation of the modern computer (Randell, 1982, pp. 337-41). Indeed, Babbage reenvisioned computation in a way that that the pioneering adding and subtracting devices by inventors such as Blaise Pascal had not in the seventeenth century (Alisha, 2002, pp. 3-4). Von Neuman also saw computers in a different way; to him they were analogs to nature, and the idea of the “syntheses of automata” to “produce other automata” was a natural step in the evolution of computing (Neumann, 1966, p. 80). Although it would be over thirty years before these programs were described by Len Adleman as a “virus,” by the 1950s scientists at Bell labs were engaging in “core wars” (Young, 2006, p. 108; Dewdney, 1984, pp. 14-22; Cohen, 1987, p. 31). The goal of these viruses were to battle and overwrite each other in the “core” processor memory until only one victor remained (Cohen, 1987, pp. 22-23). In these early efforts, programmers saw themselves, as envisioned by Von Neumann, as creating analogs to life and this game was merely an extension of the Darwinian struggle of life; hence, one of these early “core war” viruses was named “Darwin” (McIlroy et al., 1971). Indeed, Adleman’s mentee,
Fred Cohen, begins his seminal tome on computer viruses by analogizing computer viruses to viruses in nature—even in their very components (Cohen, 1986, p. 5). For early computer designers and programers, this was more than metaphorical license—they envisaged computers operating in naturalistic ways.

The military soon took interests in these efforts to create autonomous programs that could wreak havok on a computer. By 1967, the government had commissioned a study by the RAND corporation on computer security, which included “infiltration attempts through the software system” (Peterson & Turn, 1967, p. 297; Young, 2006, p. 108). By 1969, the Defense Department’s Advanced Research Projects Agency (ARPA) had created ARPANET, the predecessor of the modern internet, to facilitate the communication and interaction of computers and users over distances (Morley & Parker, 2009, p. 322). Although the virus would fundamentally remain the same, this leap forward in technology would radically change the ways by which they could be delivered. A year later, ARPA would publish a groundbreaking report on the security vulnerabilities in networked computers that contained classified documents (Ware et al., 1979). The report discusses for the first time “trap-doors” created by programmers to bypass safeguards and easily insert files (Ware et al., 1979). Exploiting these known and other unknown vulnerabilities are known as “zero day” attacks, since they are before the first day when the security flaw has been fixed (Nahari & Krutz, 2011, Chapter 8).

The first computer virus to spread across ARPANET was the Creeper virus, which was written and released in 1971 (Staedter, 2011). Continuing the benign tradition of earlier viruses, the virus would post “I’m the Creeper. Catch me if you can!” and then copy itself to another computer (Staedter, 2011). Many would classify this program as a “worm” rather than a virus, since it does not attach itself to another program and relies on
a network for transmission (Chen & Robert, 2004, p. 2). The term worm comes from the fictional work *Shockwave Rider* by John Brunner where a character releases a ubiquitous, self-perpetuating virus that will keep going even if parts of it are destroyed, like a tapeword (Shoch & Hupp, 1982, p. 1). Despite this lexiconical distinction, a worm would best be called a *worm virus*, in the sense that it still fulfills the Von Neuman vision of a self replicating program, despite its increased functionality.

It was in 1988, though, that the world received its first shocking introduction to the power of viruses. A Cornell student named Robert Morris infected computers at MIT with a worm he created; the eponymous Morris Virus then spread like a wildfire on the ARPANET and forced institutions to shut down the electronic mail to slow its spread (Filiol, 2005, pp. 259-66). Institutions were infuriated by the downtime and damage the virus caused, Morris became the first person to be convicted under the Computer Fraud and Abuse Act of 1986 (Denning et al., 1994, pp. 73-74; *United States v. Morris*, 1991). Even if Morris’ intent was as benign as he claimed (a mere computer security test that went wrong), he had demonstrated the awesome power that these self-replicating programs could have, and the world would never be the same (Denning et al., 1994, p. 74).

Three years later, the consequences of an increasingly computerized infrastructure became all too clear. In April 1991, five hackers from the Netherlands managed to penetrate US Department of Defense computer systems prior to the first gulf war and attempted to sell the information they gathered to Sadam Hussein (Delibasis, 2007, pp. 30-31). Even though Hussein declined to purchase the information, the power of this new form of warfare became undeniable (Delibasis, 2007, pp. 30-31). US forces themselves contemplated using cyberwarfare methods to disable the air defenses of the Iraqis, but
General Norman Schwarzkopf found the idea of sending in a team of hackers to a seized radar station to be too risky (Clarke & Knake, 2010, p. 9). Although unconfirmed, some have claimed that an attempt to disable the Iraqi air defenses did occur through an infected printer bought from France (Delibasis, 2007, p. 32). In the second Iraq war, a much more sophisticated approach was used. An email was sent out through the system informing Iraqi officers to surrender and abandon their equipment or face the overwhelming force of the United States; this psychological ploy proved a canny and successful move with many of the officers following the instructions and neatly parking their vehicles in formation before abandoning them (Clarke & Knake, 2010, pp. 9-10). This change reflects not only a change in US attitudes towards Cyberwarfare but also an increase in the ability and sophistication of its systems and personnel to wage such a war.

From Morris’ purportedly well intentioned worm to the “cyber shots” fired in the first Gulf war, the international stage was set for a new kind of war. Computer attacks would go where no bomb could. A new age of clandestine and open warfare would commence. As the internet globalized and expanded from Western countries and scientific communities to become a truly global phenomenon, Russia would become one of the key players in the struggle for cyber warfare capability and dominance. During the Soviet Union, progress in the fields of computers was hindered not only by shortages in materials but also by an ideological distrust of computers (Troegemann et al., 2001, pp. 16-17). Stalin himself declared Computer Science to be bourgeois science (Kittler, 2006, p. 182). With the Soviet nineteenth century preoccupation with the Marxist view of the perfected laborer, the computer was an unnecessary addition to this ultra-efficient socialist worker (Troegemann et al., 2001, p. 17). Even so, the Russians did find they needed computers for their military and space programs, so they either reverse
engineered American computers or engaged their Eastern European states in producing custom models (Ceruzzi, 2003, pp. 11-12). The Soviets would lag behind their American counterparts so much so that the first onboard computer guided manned space flight did not occur until June 1980 (Gerovitch, 2003). Despite this lag, Russian programmers quickly emerged after the Soviet Union’s collapse to be some of the best in the world. By the twenty-first century, Russian schools could beat prestigious US Universities such as MIT in programming contests (Lombardi, 2006). Further, Russians account for about 35% ($2.5-$3.7 billion) of global cybercrime revenue, yet only accounted for 1% of the global information technology market (Galeotti, 2011). Dr. Mark Galeotti attributes this to large cohorts of Russians with world-class mathematical and computer skills without the jobs to match them—a job market Russia’s mere 1% of the global information technology market implies (Galeotti, 2011).

One of the first major Internet attacks originated from Russia was by Vladimir Levin in 1994 (Corrin, 2009; Gup, 2003, p. 144). Levin was able to use security vulnerabilities in Citibank’s money transfer system to steal millions (Gup, 2003, p. 144). Despite being convicted, his successful hack served as an exemplar for the vast amounts of money that could be made through illicit activity online. During this same time, Russia was launching its first war against rebels in Chechnya (Menon, 2000, p. 32). President Boris Yeltsin believed the conflict would be over by early May, but by employing guerilla tactics, the rebels were able to humiliate the army of the former superpower (Seierstad, 2008, pp. 42-43; The New York Times, 1999). By 1999, Yeltsin enjoyed only a six percent approval rating and would be the first president of the post-Soviet Russia to resign (Seierstad, 2008, p. 61; Treisman, 2008, p. 1). Before he had left office, though, Yeltsin had started the second war in Chechnya, and his successor, Vladimir Putin, would
be charged with deciding whether to accept the Chechens’ demands or continue the fight (Seierstad, 2008, p. 61; Menon & Fuller, 2000, p. 32).

One of the reasons that the rebels, apart from their military effectiveness, had affected Yelsin’s popularity so much was their sophisticated use of the internet to both promote their cause and demoralize the Russian public (Billo & Chang, 2004, pp. 113-14). Chechens would post news about the conflict as well as videos and pictures of attacks (Billo & Chang, 2004, pp. 113-14). Indeed, the Chechen use of the media prefigured many of the techniques that would later be used during the second US Iraq war (German, 2007, p. 132). Although the first war was seen as an attempt by the weak Russian state to keep its fragile regions together, the second war was portrayed as an internal security matter and a fight against terrorism—with Putin even informing President Clinton that al-Qaeda was operating inside Chechnya (Smith, 2012, pp. 50-51).

Unlike the first war, the Kremlin wanted to control the information flow this time and engaged in its first known cyberwarfare against the rebels by attacking linked websites (Billo & Chang, 2004, pp. 113-14). The rebels responded by creating mirrors and allowing materials to be downloaded and posted elsewhere (Billo & Chang, 2004, p. 114). This electronic war finally came to the surface in a very public way when individuals linked to the Russian government allegedly launched a denial of service attack on one Chechen site while hacking into and deleting another one during the Russian storming of a Moscow theater where Chechen forces were holding hostages. After the Chechens moved the information to new sites, the Russians once again attacked the new locations (Billo & Chang, 2004, p. 114).

Russia’s intent to train legions of cyberwarriors is clear, as shown by their creation of the Voronezh hacking school which is by some estimates one of the biggest in
the world (Clarke & Knake, 2010, pp. 63-64; Galeotti, 2011). Russia also trains hackers through its excellent technical universities, such as the Siberian Tomsk University (Rainsford, 2010). Although hacking is not officially taught, a campus culture exists where students battle each other searching for security vulnerabilities in their systems (Rainsford, 2010). Yevgeny Kaspersky, one of the world’s leading computer security experts, notes that although the majority of cyber attacks are from Asia and Latin America: “Russian attacks look more professional. The malware and design is more complicated and more technical...I think it's thanks to Russia's technical education. Its graduates are probably the best [hackers]” (Rainsford, 2010). Indeed, the Russian hacking capability is undeniable. Russia in many ways uses this power to intimidate its neighbors.

Countries that were once part of the Soviet Union, such as Estonia, are the most frequent targets of these harassments. Estonia, like many of these countries, has many citizens who are ethnically Russian, but Estonia’s share is particularly high at over one-quarter of the whole population (Estonian government, 2010). Many Russian Estonians do not even have Estonian citizenship (BBC, 2007b). Further, Ethnic Estonians still feel resentment for the Soviet Union’s attempt to “russify” Estonia by promoting migration by Russians to their country and making school instruction in Russian (Estonian government, 2010; Brown, 2012, p. 202; BBC, 2007b). In 2007, these tensions all came to a head when a monument commemorating the Russian dead of World War II in the center of Talinn was slated to be moved (BBC, 2007b). The decision sparked the first major riots in Estonia in 30 years and led the ethnic Russians to clash with the police and other demonstrators—leaving many injured and one person dead (Ehala, 2009, pp. 139, 142-43; BBC, 2007b). A war of words erupted between the Russian and Estonian governments with Russian Foreign Minister Sergei Lavrov saying the move resulted from
a “blasphemous attitude towards the memory of those who struggled against fascism” while Putin called the German Chancellor to express his “serious concern” (Blomfield, 2007; BBC, 2007b).

Beginning on April 27, 2007, one day after the Estonian government moved the Talin war monument, the government websites of Estonia as well as its internet infrastructure endured three weeks of cyber attacks (Geers, 2008). Estonian officials immediately pointed to the Kremlin as being the originators of the attack (BBC, 2007a). Even though the attacks were linked to at least one Russian government IP address, the link is difficult to prove, since infected computers of innocent users can attack without their knowledge (Anderson, 2007). The attacks, though, were effective at crippling some Estonian infrastructure. For instance, most Estonians do their banking online and the attacks caused this basic financial infrastructure to be disrupted (Geers, 2008). Following the end of the conflict, The Economist offered a sobering assessment (emphasis added):

At full tilt, the onslaught on Estonia was also of a sophistication not seen before, with tactics shifting as weaknesses emerged. “Particular 'ports' of particular mission-critical computers in, for example, the telephone exchanges were targeted. Packet 'bombs' of hundreds of megabytes in size would be sent first to one address, then another,” says Linnar Viik, Estonia's top internet guru. Such efforts exceed the skills of individual activists or even organised crime; they require the co-operation of a state and a large telecoms firm, he says. The effects could have been life-threatening. The emergency number used to call ambulances and the fire service was out of action for more than an hour. (The Economist, 2007)
Indeed, the massive scale of the attack was unprecedented and deeply alarmed NATO and EU leaders, since a member of both had been so brazenly attacked (Traynor, 2007). Even so, NATO leaders were reluctant to view “cyber-attacks as a clear military action” that would invoke an Article V collective defense response (Traynor, 2007; Geers, 2008). Ostensibly as a sign of their solidarity with Estonia and concern, NATO opened up a Cooperative Cyber Defence Centre of Excellence in Estonia the following year (NATO, 2008; A. Mitchell, 2008). Russia’s mysterious ability to conjure up armies of hackers at precisely the moment they help its policy objectives again arose as it attacked a small former member of the Soviet Union to its South.

Much like Estonia, Georgia also has a large contingent of ethnic Russians living within its borders (Minorities At Risk Project, 2006). Unfortunately, it also has two so-called frozen conflict zones in Abkhazia and South Ossetia within its borders (Beehner, 2006). In what can only be described as ill-advised, the Georgian government sought to reunify the ethnically Russian dominated South Ossetia with the rest of the country and invaded it on August 7, 2008 (The Economist, 2008). In doing so, it it killed Russian peacekeepers and managed to bring the full might of Moscow down on it (Reuters, 2008; The Economist, 2008). Five days later, in an EU brokered peace agreement, the crushed Georgian military would retreat back to its undisputed territories (Cohen & Hamilton, 2011, p. iii). This short war, though, would stand as a remarkable turning point in Russian military history. This war was the first time the Russian military used cyberwarfare to support its conventional war operations (Cohen & Hamilton, 2011, p. 40). Although its operations in nearby Chechnya were certainly done to suppress the information flow by and propaganda of the Chechen rebels, the Georgian campaign was the first time the Russian military operated a conventional campaign in tandem with an electronic
campaign targeted at government websites, local media and internet infrastructure (Cohen & Hamilton, 2011, p. 44).

The cyber attacks began on August 8 within 30 minutes of each other and ended August 11 when Russia announced a ceasefire (Cohen & Hamilton, 2011, p. 44.). Although the Estonian attack was quite sophisticated, this attack proved to be even more sophisticated with two distinct prongs. First, the hackers attacked government and media sites in Georgia (Government of Georgia, 2008, pp. 3-4). The Georgian president’s page was changed to include a slideshow comparing him to Hitler (Government of Georgia, 2008, p. 4). Likewise, official email servers went down (Cohen & Hamilton, 2011, p. 46). Further, websites of local media, such as the Georgian News Agency, went down (Government of Georgia, 2008, pp. 4-5). The Georgian government responded by shifting its websites to US hosts and using personal email addresses, like they had done until recently before the official email system had been created (Cohen & Hamilton, 2011, p. 46). Indeed, the cyber attack proved somewhat rebuffed on this front due to the screwd actions of Georgian officials. The second and far more sophisticated prong was the a “cyber blockade” (Government of Georgia, 2008, p. 5). Rather than simply launch denial of service attacks, sources claim the Russians took over the internet infrastructure and routed Georgian internet activity through Russia and blocked key internet activity coming out of it (Tikk et al., 2008, p. 11; Government of Georgia, 2008, p. 5). Indeed, this wholesale takeover of Georgia’s networks completely cut its financial system off from the world and crippled its internet infrastructure (Thibodeau, 2009). Unlike its conventional forces, which Russia proudly touts, the Russian government remains guarded about its cyberwarfare attacks and implies these attacks are by patriotic third parties (Markoff, 2008). Most experts agree this “shadowy” force behind the attack is the
Russian Business Network—a group that peddles everything from child pornography to spam with its services going to the highest bidder (Krebs, 2007; Government of Georgia, 2008, p. 5; Markoff, 2008; Cohen & Hamilton, 2011, p. 45). Indeed, costing roughly four cents a machine, these cyber mercenaries are far cheaper than conventional forces, but they can cripple enemy states economically more effectively than bombs often can (Markoff, 2008). It is unclear how far the increasingly opaque and nationalistic government of Putin is willing to go when asserting its dominance over its neighbors—even if that means collaborating with criminals.

Within Russia we see a clear escalation in the sophistication of its cyberwarfare. This is a consequence of the increasingly sophisticated attackers within Russia, whom the government uses and often trains. Russias is in a race to keep up with sophisticated cyberwarfare operations—like those in US ally Israel. This is especially true now that it has so closely allied itself with traditional Israeli enemy Syria. Unlike Russia, Israel embraced computing early on by building the Weizmann Automatic Computer (WEIZAC) in 1954-55—one of the first John Neumann IAS (Institute for Advanced Studies) Computers in the world built outside the US (Estrin, 1991, p. 318; Mirowski, 2002, p. 491). The cutting edge Von Neumann architecture used in this computer would also be the basis for modern computer architecture (Godse & Godse, 2010; Eigenmann & Lilja, 1998, pp. 1-2). By the 1960s, this small country ranked with the United States and Japan as a “world leader in software design and production” due to intensive government investment—particularly by the defense sector (Mirowski 2002, 491). By the 1990s, Israel’s computer industry was known as “Silicon Wadi” (Mirowski 2002, 491).

Although Israel does not have a hacking school as large as Russia’s, the Israeli government is determined to train hackers to defend against and attack other countries
targeting it, such as Iran (World Tribune, 2012). Unlike other nations, though, Israel has been engaging in an informal cyberwar with its enemies for over a decade, beginning with the Second Intifada in the so-called “cyber intifada” (Denning, 2007, pp. 129-30). During the second Intifada, a group of pro-Israeli hackers attacked Hezbollah’s website after several Israeli soldiers had been kidnapped; in retaliation, hackers, some linked to Hezbollah, attacked Israeli government, banking and commerce sites as well as internet infrastructure and then released the credit card information of supporters of Israel (Middle East Intelligence Bulletin, 2000; Denning, 2007, pp. 129-30). Back and forth attacks would continue with hackers attempting to crimple to the Israeli information technology sector (Middle East Intelligence Bulletin, 2000). In 2003, an internet forum linked to Hamas called for more cyber attacks on Israel by luring Israelis to virus filled pages; a year later a website called Internet Haganah, dedicated to fighting internet terrorism, was attacked to prevent its operation (Denning, 2007, p. 30). The Israeli hacker community has resorted to creative measures in fighting this back and forth war. One group of Israeli students created a program called “Patriot” which anyone can download so that their computer can be used to overwhelm websites, such as those of Hamas (Shachtman, 2009; Carr, 2012, p. 28). Anti-Israeli hackers had developed a similar tool earlier, but it did not receive wide acceptance (Racicot, 2009).

The Palestinians and Lebanese are not alone in their cyber warfare against Israel. On this virtual battlefield, Israel is being attacked by hackers from around the world—many of whom are supported by their government. Recently, a hacker linked to a Saudi Arabian hacking group engaged in a series of hacks where he released thousands of credit card numbers and eventually went after the webpages of Israeli stock exchanges (Fisher-Ilan, 2012; Messieh, 2012). Israeli hackers retaliated by releasing credit card and other
confidential information about Arabs—eventually attacking Saudi Arabian and United Arab Emirates stock exchanges (Messieh, 2012). Egyptian hackers likewise have engaged in this cyber battlefield with Israel—recently defacing Prime Minister Benjamin Netanyahu’s website (The Hacker News, 2011). Indeed, in 2008 the Egyptian Muslim Brotherhood published a Fatwa sanctioning electronic jihad (Spencer, 2008). Even Pakistanis, who normally attack Indian sites, have attacked Israeli related sites in this continuous battle against this electronically besieged state (Jamshed, 2008). Israel’s most fierce cyber rival is Iran. Iranian hackers have targeted Israeli infrastructure, such as their banks (Mezzofiore, 2012). Iran’s Republican Guard set up a division devoted to cyberwarfare in 2010 with a budget of $76 million and claims to have a million members in its “cyber militia;” it now even claims to be increasing its budget for cyberwarfare to $1 billion (Danchev, 2012; Waterman, 2012). Israeli hackers have attacked Iranian websites to replace them with pictures of Israeli flags and even brought the state television channels down (Lappin, 2012). Indeed, the US and Israel virtually declared cyberwar on Iran to stop its nuclear program before the Obama’s nuclear agreement (Sanger, 2012b). In fact, Israel’s most effective and intense cyberwarfare efforts have been to stop its neighbors from getting nuclear weapons.

Syria has historically had a very tense relationship with Israel and been allied with the Soviets and Russia. Believing that the Israelis might attack it to overthrow its regime due to Soviet misinformation, Syria was one of the major instigators of the Six Day War (Ro’i, 2008, pp. 5-6). During the final hours of the conflict, Israel was determined to seize as much territory as they could—particularly the Golem Heights from which Syria could reign down weapons (Broyles, 2004, pp. 50-53). The area is still disputed, and the border of the territory with Syria is supervised by UN peacekeepers (Wiegand, 2011, p. 29;
United Nations, 2011). After ominous signs of Syria’s attempts to build a nuclear program with the help of the North Koreans and Iranians since at least 2003, Israel decided that it was time to stop its enemy to the north from becoming another nuclear power (Wright & Warrick, 2008; Niksch, 2010, pp. 20-21). In fact, the US government would later state that the reactor was nearly operational when the Israelis bombed it and that it believed that the Syrians were indeed attempting to build a non-peaceful nuclear program—much like the North Koreans have (Rosenkrantz, 2008; Niksch, 2010, p. 21).

On September 5, 2007, a squadron of Israeli airplanes would leave Ramat David Air Base and enter cyberwarfare legend as part of “Operation Orchard” (Cha, 2012, Chapter 7). These were not stealth planes; in fact, they were bulky and easy to detect (Clarke & Knake, 2010, pp. 4-5). Even so, the Israelis pierced the several billion dollar Russian air defense system without losing a single plane (Clarke & Knake, 2010, p. 5). Although invisible to the majority of the air defense system, they still had to evade a few missiles and destroy a radar station at Tall al-Buad (Cha, 2012, Chapter 7). Soon the al-Kibar facility was in ruins, and the Israelis had made it very clear to the Syrians and their neighbor, the Iranians, that nuclear weapon development would not be tolerated (Cha, 2012, Chapter 7). According to Richard Clarke, a former high level official in the Washington security establishment, there are three possible ways that the Israelis pulled off this cyberwarfare feat: a drone that sent a digital signal to the radars which caused them to malfunction, Israeli agents had planted or knew of a “trapdoor” within the code operating the defense systems or the Israelis physically spliced into the fiber lines that controlled the defense system and used that to infiltrate the network (Clarke & Knake, 2010, pp. 6-8). Whatever the method, the Israelis had successfully intergrated conventional and cyberwarfare operations with unprecedented skill and sophistication.
Many believed this attack on Syria was as much or more a warning to Iran to cease its attempts to create a nuclear bomb (Clarke & Knake, 2010, p. 3). This nimble and successful use of cyberwarfare no doubt both inspirational and disconcerting to the Russians—given that the Israeli had defeated the defense system.

Back even in 2009, experts believed that Israel would try to wage cyberwarfare on Iran’s nuclear facilities before attempting to bomb the buildings deep within Iranian territory (Williams, 2009). In late 2010, it emerged that Iran was having serious issues with its centrifuges and that it was having to replace many of them as they malfunctioned (Jahn, 2010). Although the Stuxnet virus had been discovered by then and thought to be the cause, its sibling, the Flame malware, had not yet been identified (Zetter, 2012b; Jahn, 2010). To call either of these cyberwarfare weapons groundbreaking is an understatement. They were revolutionary. Although discovered later, Flame is likely how the developers in the United States and Israel gathered much of the intelligence to know exactly how to target the Iranian systems (Zetter, 2012a). Another component called a “beacon” was likely used also to map the Iranian centrifuge plant and discover the exact hardware and methods the Iranians used to control the plant (The New York Times, 2012). The remarkable agility with which these components were placed into the Iranian systems and then exploited has brought cyberwarfare to a whole new level.

Flame is rightfully called “one of the most complex cyber weapons yet,” “the world’s most dangerous malware” and a “super cyber-weapon” and demonstrated to Russia the power cyberwarfare could yield without a single shot being fired—weapons arguable more powerful than mere bullets and bombs (Greenwood, 2012; Aleem, 2012; Goessl, 2012). Flame is related to Stuxnet in several of its components and how it
operates (Bitdefender Labs, 2012b). When experts discovered Stuxnet, they were likewise stunned at its sophistication (Dang, 2011; Nachenberg, 2012). As a professor at Stanford and leading engineer in the industry said, “Stuxnet bypassed everything we had” (Nachenberg, 2012). Stuxnet is indeed remarkable. It acts like a virus by parasitically attaching itself to programs (Nachenberg, 2012). It is a worm because of how it spreads itself across the network (The New York Times, 2012; Nachenberg, 2012). It is a Trojan Horse because it masquerades as something it is not by using the digital signatures of leading companies, like Realtek; this is an unprecedented level of sophistication for a Trojan Horse due to the fact the encryption keys to create these signatures are closely guarded (Weiss, 2010; Nachenberg, 2012). Indeed, Stuxnet is so sophisticated that it is 50 times the size of a normal piece of software that would perform similar objectives; it has seven ways it can spread itself (Nachenberg, 2012). Among these methods are: using openly shared files between computers, using a vulnerabilities in the way Windows computers can speak to each other, attacking Siemens Programmable Logic Controllers (PLCs), changing data files to infect the computer on opening and usb drives (Nachenberg, 2012). Further, it can update itself through peer to peer sharing over a network; this effectively means only one program needs to be on a computer accessible to the internet for the virus to update (Nachenberg, 2012). To exploit many of the flaws in Windows that Stuxnet exploits, you would need to look at the Windows source code or else reverse engineer it, which would take years.

The actual functioning of Stuxnet is also extremely sophisticated. First, it operates across two operating systems and programming languages to infect the Siemens PLCs; this means it can spread through Windows and infect the PLCs connected to those Windows PCs (Nachenberg, 2012). Second, it inhibits different behavior when
confronted with different anti-virus software (Nachenberg, 2012). This is so it can evade detection for as long as possible. Third, it attacks the centrifuges in such a way as to avoid detection and still damage them (Nachenberg, 2012). It does this by measuring the operating speed of the frequency converters for 13 days and makes sure it is spinning at the right rate and is indeed a nuclear centrifuge, which spins at a specific very high rate (Nachenberg, 2012). It then raises the spinning rate to 14,100 Hz for 15 minutes and goes dormant for 17 days (Nachenberg, 2012). It then slows the spinning to 2 Hz for 50 minutes, but during these changed speeds it won’t allow it to be shut down (Nachenberg, 2012). It also sends back fake recorded data so that it is difficult to understand what the problem is (Nachenberg, 2012). The precision and ingenuity of Stuxnet is remarkable. Variants of Stuxnet that are aimed at different problems, but the proof concept had wide ramifications—if you can attack centrifuge industrial controllers than you can attack modern industrial controller for power plants and other basic infrastructure—like waste water treatment (Bencsáth, 2011). Russian hackers—any hackers with enough sophistication—could cripple a country—at least temporarily.

Israel and the US became so dominant in the Cyber domain that attacks on Iran became almost abnoxious. During a recent attack, infected computers would allegedly begin randomly playing the AC/DC song “Thunderstruck” (Matyszczyk, 2012). According to one source, a frustrated Iranian scientist wrote, “There was also some music playing randomly on several of the workstations during the middle of the night with the volume maxed out. I believe it was playing ‘Thunderstruck’ by AC/DC” (Faircloth, 2012). Despite the humorous aspects of this, it demonstrates the incredible domination that nation states like Israel and the United States can yield with sophisticated cyber weapons.
Russia has gained extremely high competence in the cyberwarfare sphere in part as a consequence of its competition with the US and its allies—like Israel—and in part due to its indigenous high degree of technical knowledge and expertise. While the Georgian war showed weaknesses in the Russian military in some respects, it also showcased their emergent cyberwarfare capability. Indeed, General Gerasimov recognized the learning that occurred after the Georgian war in terms of force projections outside of Russia and likely used the force modernizations afterwards as an opportunity to advance his own vision for a stronger, modern Russian fighting force that use dominates its enemies in cyberspace and information spheres both before, concurrent with and even in lieu of the deployment of kinetic operations (Bartles, 2016).

Faced with a low birthrate to provide conscripts and recruits, an obstinately corrupt armed forces and the task of protecting a country that spans 11 time zones from central Europe to northeastern Asia, Gerasimov’s approach provides for leveraging small and well funded special operation and military intelligence units to project force in cyberspace at a relatively low cost and low manpower requirement make sense for Russia. Gerasimov is arguing for a light footprint and technologically sophisticated military of the future pared with the threat and ability to provide overwhelming conventional and nuclear forces—if needed (Gerasimov & Bērziņš 2017).
Chapter IV.
Gerasimov’s Importance

Much of the analysis of Gerasimov seems to at one point or another fall into the inevitable debate over whether or not he is the new “great man” of the Russian military of our times. Western historical narratives too often pivot from one great man—sometimes woman—to another regardless of the known weakness of this approach. One recent article in FP wondered aloud if Donald Trump was a “great man” and mused if historians should admit the potential validity of this approach:

The imminent ascension to the U.S. presidency of Donald Trump, a man whose supporters and detractors both agree is exceptional in the context of American history, raises a question which historians and social scientists generally prefer to shy away from: To what extent does historical change depend on the actions of a handful of unusual individuals — history’s archetypal Great Men and Women — as opposed to large-scale, long-term, impersonal forces? (Bell, 2017)

While historians may cringe at the thought of returning to such historical reductionism, in the case of Russian military evolution following the fall of the Soviet Union the idea that Gerasimov is the single author of Russia’s military strategy in Ukraine is absurd. It is enough that the approach he describes—sometimes called the Gerasimov Doctrine—is largely descriptive of the Russian military’s approach in Ukraine. We can view Gerasimov as providing one of the clearest articulations of a hybrid warfare style operations modeled on Western Color revolutions and the many benefits this style of war fighting. Whether Gerasimov is a great military theorist himself is of little consequence—
he has risen to the highest echelons of the Russian government and partakes in the in
debates he ruminates on.

For maximum understanding, Gerasimov’s writings and speeches need to be
contextualized in several key ways. First and foremost, Gerasimov is said to be Defense
Minister Sergei Shoigu’s chief military advisor—in essence, a formal and informal
talisman for the long time former emergency manager turned military chief. As the FT
notes in one of the rare profiles of the enigmatic Gerasimov:

A man of few words who appears in public infrequently, Mr Gerasimov is
a general’s general, described by Sergei Shoigu, Russian defence minister,
as “a military man to the roots of [his] hair”.

Mr Shoigu, a politician-turned-general, is said to lean on the former tank
commander for military advice. “If Shoigu is an excellent air guitarist,
then it’s Gerasimov playing in the background,” according to one
anecdote. (Foy, 2017)

Gerasimov’s public speeches and writings are few and far between for such a sharp mind
who holds such a high post in one of the largest militaries in human history. These
writings no doubt reflect his own views on military matters and the advice he gives
Shoigu.

Originally appointed by Yeltsin, General Shoigu is a survivor and confident of
President Putin and has served in the Russian government from its beginning as a post-
Soviet state:

But Mr Shoigu is much more than Russia’s latest defence minister. At 60,
three years younger than Mr Putin, he is the longest-serving member of
the Russian government; his tenure stretches back to 1990, before the collapse of the Soviet Union, when Mr Putin was still toiling in obscurity in the St Petersburg mayor’s office. He made his name at the Ministry of Emergency Situations (MChS), a semi-militarised rescue service with a wide remit that he built himself and led for nearly 22 years. By skilfully navigating Russia’s Byzantine bureaucracy, he has accrued power and popularity without making any notable enemies. “There’s no one else like him in the ruling class,” says Evgeny Minchenko, an analyst who studies the Russian elite. “It’s an absolutely unprecedented story.” (Economist, 2015)

A potential successor to Putin and confidant, Shoigu is Putin’s most trusted advisor apart from his chief of staff—virtually ensuring that Shoigu’s advise was instrumental in invading Ukraine:

Although Mr Shoigu does not belong to Mr Putin’s coterie of ex-KGB men from St Petersburg, he is a trusted insider. Mr Minchenko, who releases a widely circulated yearly report called “Politburo 2.0”, puts Mr Shoigu second in influence among Mr Putin’s associates, trailing only his [now former] chief of staff, Sergei Ivanov. When big decisions like the operations in Ukraine or Syria are made, Mr Shoigu is indispensable. His combination of loyalty, competence and popularity also makes him one of a handful of potential successors to Mr Putin. (The Economist, 2015)

It is inconceivable therefore that Gerasimov himself did not both directly and indirectly influence the Russian decisions and methods by which to wage war against Ukraine.
Second, Gerasimov is Chief of the General Staff of the Armed Forces of the Russian Federation and First Deputy Minister of Defense of the Russian Federation. He literally is one of the chief planners of the Russian military strategy he is discussing in his famous article The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations. As one scholar discusses his role (footnotes omitted, emphasis added):

Although the Russian Security Council is the chief proponent of Russian strategy, the Chief of the Russian General Staff does sit on council, bridging operational art to the national security strategy. The General Staff does far more than just plan operations. It also has responsibility for the use of “foresight” to develop the theory and practice of future war. In Russian military thought foresight is directly linked to military science, with military science being the science of future war. The General Staff’s responsibility to predict the nature of future war makes it the logical place (in the Soviet/Russian system) for doctrine and capability development for the entire Ministry of Defense.

Just as important as what the General Staff does is what the General Staff does not do. It does not have operational control of the force. Although there were Goldwater-Nichols-like reforms that removed operational control from the branch chiefs (Ground Forces, Air Force, etc.) and placed the operational control of most forces with regional commands, little has changed with the
General Staff’s role as operational planners and capability and doctrine developers since Soviet times. (Grau & Bartles, 2016, p. 11)

Gerasimov is a participant, influencer, and articulator of a debate within the post-Soviet military as it moves beyond antiquated Soviet warfighting methods and equipment to compete with the highly advanced methods and equipment of the West. Gerasimov’s *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations* is based on a speech made a mere 3 months after Gerasimov’s 2012 appointment as Chief of the General Staff and First Deputy Minister of Defense (Foy, 2017). It represents the General’s first foray into this debate from this senior post—no doubt an influential articulation representing the thinking he expressed himself in internal discussions.

Despite the obvious importance of Gerasimov’s writings and approach, he is often dismissed as merely repackaging the approaches used in KGB active measures and suggested by others as well in debate over what future Russian warfighting should be. Gerasimov’s article is well within the sphere of the ongoing debate within the Russian military over different conceptions of Russia’s new fighting approach, whether it is General-Lieutenant A. V. Kartapolov “new-type war” (NTW) or General-Lieutenant S. A. Bogdanov and Reserve Colonel S. G. Chekinov’s “new-generation warfare” (NGW)—a term that has fallen now out of favor (Thomas, 2016, pp. 554-56). Indeed, the roots of this debate stretch into the 1990s as the Russian military transition from the Soviet one that preceded it:

Bogdanov and Chekinov appeared to be restating many of the thoughts of retired (now deceased) General-Lieutenant Vladimir Slipchenko, who was
a driving force for new thinking in Russia in the 1990s and the early part of the next century. He wrote often on what he referred to as ‘sixth generation warfare’, or noncontact warfare, which would be based on high-technology weaponry and systems able to maneuver in small groups. Slipchenko’s work may be considered as a (or the!) most important source behind much of the new-generation warfare thinking and postulating of Bogandov and Chekinov. In fact, in 2013, a Slipchenko-authored article appeared posthumously in the Russian military publication Army Journal. It discussed Slipchenko’s description of planetary warfare and several other new-generation warfare concepts.

(p. 555-56)

These vague conceptions of modern warfare are constantly in flux, though. Representing more a direction of military thought than a hardened school of military theory. The use of special operations, advanced weapons, information warfare and cyber attacks are all elements of the various positions advanced within the Russian general staff—some more heavy on conventional and kinetic operations while a method like Gerasimov’s relies primarily on the power of non-conventional weapons like information and political pressure (Thomas, 2016).

Western academics, journalists and scholars seem to be falling victim to a bizarre idiosyncrasy of the Russian Military that is a carryover from Soviet Times to provide international cover for controversial approaches—claim these tactics and strategies are really Western tactics:
Russian military officers (to include Gerasimov) refute the use of hybrid methods by the Russian military, stating clearly that this is a Western method of conducting modern war. Other officers make the same claims about NGW and NTW, initially stating that these are Western concepts (an argument Westerners have not made!). Clearly Russia has studied all three and learned from an examination of the concepts, eventually describing their components and how to counter them. This appears to be the use of an old Soviet method, that being to describe how another country conducts war when actually the description is of Russian methods. (Thomas, 2016, p. 555)

Any critique of the methods by other countries is spun as hypocrisy. In a sense these Russian methods are a dark reflection of Western ideas, because they are an attempt by Gerasimov and the Russian military at large to use what they see as Western military methods against the West and its allies. Even so, Gerasimov’s cynical and distorted articulation has made this “hybrid war” method a distinctly Russian articulation.

One Russian propaganda outlet advanced the theory hybrid warfare in Russia was simply an invention of exiled fascists—deriding the West’s portrait of Gerasimov as the arch villain of the Russian military’s forays:

[T]he idea of 'hybrid warfare' is anything but new. "In Russia, the idea of the 'part-war' was something on which thinking began a very long time ago." An important theoretician on this type of war was ex-soldier and academic Evgeni Messner (1891-1974), "one of the most important representatives of military thought among the Russian diaspora."
An officer in the Imperial Russian Army, Messner fled Russia after the victory of the Bolsheviks, settling in Yugoslavia, and collaborating with the Nazis during the Second World War against the Red Army. His best-known publication 'Mutiny, or in the Name of the Third World War,' predicted that the wars of the future would be fought by terrorists and special forces, with states using subversion and organizing revolutions, rather than traditional warfare, to gain power and influence.

Messner wrote: "Future wars will not be fought on front lines, but throughout the entire territories of both opponents, because behind the front lines political, social, and economic fronts will appear; they will fight not on a two-dimensional plane, as in olden days, not in a three-dimensional space, as has been the case since the birth of military aviation, but in a four-dimensional space, where the psyche of the combatant nations will serve as the fourth dimension." (Plehanov, 2017)

Military blogger Mark Galeotti’s “apology” for evidently coining the term “Gerasimov Doctrine” gave Russian propaganda yet another chance to mock the West for believing Gerasimov’s own words:

Even as he backtracked from the ‘Gerasimov Doctrine,’ Galeotti maintained that Russia was still practicing the policies described in the speech, subverting Western democracy and institutions as the only way to compete “with a larger, richer coalition of democracies” represented by NATO. President Vladimir Putin, he claimed in the Foreign Policy essay,
was “largely wrong, but not entirely so” about the threat to Russia from the West, to which US actions have “inadvertently contributed.”

It seems this was Galeotti’s way of saying he only got a little hyperbolic with the title, but the rest of his “expertise” on Russia still stood. While it is not hard to sound reasonable about Russia in comparison to, say, the corner of Twitter that has gathered around Louise Mensch, Galeotti still has miles to go. (RT, 2018)

Galeotti’s attempt to maintain relevance in the debate over Russian military approaches in the war did little more than distract Western militaries from Gerasimov’s importance as a military thinker and leader.

Third, Gerasimov’s approach aligns with rivalry between Russia’s military and civilian intelligence apparatuses with military intelligence seeking more funding and a larger role. This rivalry grew so intense in the 2016 election that civilian FSB intelligence agents informed US intelligence about military GRU operations:

Reiter delved into the mystery of why the men were charged with, of all things, passing information to the CIA about the Russian cyber-attack. According to Reiter, they had been set up by a rival faction in Russian military intelligence, the GRU. The rivalry, which Soldatov and Borogan had also reported on, centered on securing both the prestige and budgetary funds that came with penetrating U.S. government cyber-defenses. This had previously been the exclusive domain of the FSB—once run by Putin—and the GRU was trying to muscle in on the FSB’s territory and
money. A side effect of this internal rivalry, Reiter concluded, was how the Americans discovered the hack. (Ioffe, 2017c)

This rivalry is why Gerasimov’s use active measures to exploit social fractures sounds so much like the civilian intelligence operations of times past—such as the KGB’s efforts during the civil rights movement (Ioffe, 2017b). Indeed, if the military can control the large-scale information campaigns and receive the funding to do so, it can integrate them into broader military strategies. It appears during the 2016 election, it was Russia’s military intelligence did far more damage—as a July 2018 indictment of military officials involved in the Guccifer 2.0 campaign shows:

In or around 2016, the Russian Federation (“Russia”) operated a military intelligence agency called the Main Intelligence Directorate of the General Staff (“GRU”). The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted largescale cyber operations to interfere with the 2016 U.S. presidential election. (Department of Justice, 2018)

Their Hillary Clinton email hack and release of emails is thought by many to have changed the course of the election while the FSB efforts through the Internet Research Agency likely had minimal effect other than perhaps polarize more those who were successfully influenced by them (Silver, 2017). Russian military intelligence inflicted a wound that Clinton never recovered from and which was likely made fatal by the infamous Comey letter (Silver, 2017). For Gerasimov, these measures—once mostly the province of civilian intelligence agencies—are (in fact) the most powerful than the
traditional kinetic weapons militaries fight with: “The very ‘rules of war’ have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness” (Gerasimov, 2016b, p. 24). Gerasimov is here to harness these techniques and use them militarily, so it is inane to argue whether or not he invented them. Gerasimov and his colleagues are trying to convince Putin—infamously a KGB spy—the military should be at the vanguard of efforts to counter color revolutions and destabilize the governments of Russia’s enemies.

Finally, if one were to ask in a deep and historical sense the origin of the broadest outlines of Gerasimov’s approach, the answer might surprise many. In many ways, Gerasimov’s deepest theoretical underpinnings can be found in the trenches of World War I. It was there in that bloody conflagration of horror and death that European nations realized that the linear warfare methods of the past were outdated and new tactics had to be developed to break enemy lines and prevent the entrenched and devastating battles of that war (Harrison, 2010). For the Germans, this meant the use of approaches like Blitzkrieg—an attack so fast and powerful by an armored division that the enemy could not mount effective defensives quickly—and for the Soviets this meant the deep operation—attacking the enemy at every point of the battlefield and its ability to support and maintain engagement at the line of contact (Habeck, 2003; Harrison, 2010). It was these methods and approaches developed during this period that would eventually help the Soviet’s win World War II along with the allied troops—in spite of the fact many of these geniuses were murdered or exiled by Stalin’s fanatical regime. Gerasimov himself notes his admiration for these persecuted military geniuses and views those who are pushing back against the modernization he is suggesting as anachronistic:
The state of Russian military science today cannot be compared with the flowering of military-theoretical thought in our country on the eve of World War II.

Of course, there are objective and subjective reasons for this, and it is not possible to blame anyone in particular for it…. [These military theorists] were extraordinary personalities with brilliant ideas. I would call them fanatics in the best sense of the word. Maybe we just do not have enough people like that today. People like, for instance, Georgy Isserson, who, despite the views he formed in the prewar years, published the book New Forms of Combat. In it, this Soviet military theoretician predicted, “War in general is not declared. It simply begins with already developed military forces. Mobilization and concentration are not part of the period after the onset of the state of war as was the case in 1914 but rather, unnoticed, proceed long before that.” The fate of this “prophet of the Fatherland” unfolded tragically. Our country paid in great quantities of blood for not listening to the conclusions of this professor of the General Staff Academy.

What can we conclude from this? A scornful attitude toward new ideas, to nonstandard approaches, to other points of view is unacceptable in military science. And it is even more unacceptable for practitioners to have this attitude toward science. (Gerasimov, 2016, pp. 28-29)

Gerasimov makes clear he is casting his lot with the “fanatics” who helped the Soviets win World War II and is urging the Russian military to turn the lessons of the color
revolutions into a modern approach that can defeat Western militaries at their own game—deep operations that reach far beyond and in some ways usurp the traditional points of contact:

Frontal engagements of large formations of forces at the strategic and operational level are gradually becoming a thing of the past. Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals. The defeat of the enemy’s objects [objectives] is conducted throughout the entire depth of his territory. The differences between strategic, operational, and tactical levels, as well as between offensive and defensive operations, are being erased. (Gerasimov, 2016b, p. 24)

For Gerasimov—as his opening line suggests in its echo of Isserson—wars are not declared with clear beginnings. The battlefield is not limited by time and space with the opening salvos likely happening in the information sphere long before any military points of contact: “In the twenty-first century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template” (Gerasimov, 2016b, p. 24). Indeed, modern technology enables the military to extend the deep operation in ways that even the ingenious “fanatics” like Isserson could not imagine.

Given the US’s technological superiority, much higher military spending, and an economy more than 10 times the size of Russia’s, asymmetrical, non-linear engagement especially in the information sphere allows a country like Russia to dominate the US and leave it reeling:
The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy. In North Africa, we witnessed the use of technologies for influencing state structures and the population with the help of information networks. It is necessary to perfect activities in the information space, including the defense of our own objects [objectives].

(Gerasimov, 2016b, p. 27)

Deep operations—like those regarding the Clinton emails—have allowed Russia to wage war on the United States with only weak pushback while gained a president who feels even acknowledging these efforts happened will delegitimize his presidency and help his foes. This can be seen no better than Trump’s response to questions about Russia’s actions during the election that brought him to power:

My people came to me, Dan Coats, came to me and some others, they said they think it’s Russia. I have President Putin. He just said it’s not Russia.

I will say this: I don’t see any reason why it would be. But I really do want to see the server but I have confidence in both parties.

I really believe that this will probably go on for a while, but I don’t think it can go on without finding out what happened to the server. What happened to the servers of the Pakistani gentleman that worked on the DNC? (Irish Times, 2018)

During the press conference, Trump practically made the arguments for Putin that Russia had not interfered. Having a US President feel obligated to support a bald-face lie—against both the opinion of the Justice Department who just indicted 12 military
intelligence figures and an intelligence community that warned the prior administration as well—will likely go down in history as one of the great information warfare victories in modern times—despite the fact Trump has somewhat backtracked on his comments (Wagner & Sonmez, 2018). Russia has beaten the nation who both invented the internet and social networks by using these technologies far better than the US ever has in a military sense—despite Gerasimov and much of the broader Russian military’s belief that social media based civil society efforts (especially in color revolutions) are simply US intelligence operations (Cordesman, 2017; Gerasimov, 2016b; Bouchet, 2016). Ironically, Russia is beating the US at a game they believe the US invented when—in fact—it is Russian who are the true innovators in this realm.
Chapter V.
Countering Gerasimov through De-Escalation

Much of Ukraine’s efforts are devoted to increasing its conventional forces as well as launching efforts to counter the cyber and information wars. It should be remembered, though, the approach Gerasimov first articulated in *The Value of Science is in the Foresight* anticipates an escalation of violence that the manipulating government can use as a pretext for intervention. If Ukraine were to launch a massive effort to expel the Russian backed separatists and the Russian military supporting them in Ukraine, Gerasimov would respond in kind—launching a huge military campaign in a “peacekeeping” operation that would lead to a unending frozen conflict, independence of the captured territory or outright annexation. Each of these options would be dark reflections of what Russia sees as the damaging and hypocritical campaigns of Western powers and the US in the Balkans, Middle East and around the globe. One option for countering Gerasimov’s approach is descalation—realizing the cost of escalation in the war and fragility of Russia itself. One potential solution has been applied to gun violence in Chicago.

Gun violence in Chicago is famously horrific and ubiquitous in the poorer parts of the City—often bleeding into the wealthier parts due to its sheer scale. A beautiful and dynamic city, gun violence has nonetheless earned its names like “Chiraq”—referring to the fact that gun violence has rendered parts of the city as dangerous as Iraq to the eyes of some (McKissack, 2017). Many metaphors exist for violence and ways to address it, but violence as a disease spreading has proved one of the more valuable ones on the streets of Chicago—spurring one of several interventions that helped bring Chicago’s murder rates
down by 16% in 2017 (Park, 2018). This section will argue that this approach of treating violence as a disease—would be an effective intervention in the war in Eastern Ukraine and help bring down the civilian deaths there.

In the war in Eastern Ukraine, the combatants and primary parties are Ukraine, Russian-backed separatists and Russia itself—given that its military (especially Military intelligence and Special Operations) is and has been in direct combat with the Ukrainian military (Peterson, 2017). The Russians appeared to believe that an insurgency of ethnic Russians only lightly supported by Russian Military Intelligence and Special Operations could overcome any Ukrainian resistance to an autonomous status and eventual annexation of large swaths of Eastern and Southern Ukraine, but with the violent and fierce battle in Sloviansk, the Ukrainians made clear that Ukraine had made its nonviolent stand in Crimea and from now on would fight over every meter of its territory Russia was trying to claw back through its proxies and military parading as proxies—regardless of whether it would have to fight rebelling Ukrainians as well (The Economist, 2014b). Within a year, the tide had turned in favor of the Russian back separatists—now supplied with anti-aircraft weapons capable of shooting down even airliners, large contingents of Russian soldiers and heavy weapons—and they dealt the Ukrainian military as stinging defeat in the Battle of Debaltseve as they tried to gain as much territory as possible before another shaky ceasefire—known as Minsk II—was implemented under pressure from key secondary and third parties—including France, Germany and the United States. Under the agreement, the Organization for Security and Co-operation in Europe (OSCE) monitors the ceasefire line and reports violations—a now daily occurrence (Shalal, 2018).

Given the fact that Ukraine—for now—is politically committed to use the full force of its military to oppose to retain its sovereignty over its territory as it stood after
the forced occupation of Crimea and the fact that the Russian separatists would be unlikely to be able to withstand the full force of the Ukrainian military alone, the future of the conflict depends largely on Russia’s political will to continue it—since the Ukrainians cannot defeat Russia’s conventional forces and Russian military doctrine explicitly allows threat and use of nuclear weapons as their own “de-escalation” measure under the so-called “Ivanov Doctrine” (Schneider, 2017). Thus, even if the Ukrainian military undergoes a massive transformation and begins to force the separatists and the Russian military out of their country, Russia could potentially threaten or actually use nuclear weapons to force Ukraine’s military to stop. To understand the future of the Ukrainian conflict, one must understand what Russia views in its national interest—no easy task. As Winston Churchill noted in a speech a month after a German invasion of Poland that was facilitated by the Molotov–Ribbentrop Pact:

I cannot forecast to you the action of Russia. *It is a riddle wrapped in a mystery inside an enigma; but perhaps there is a key. That key is Russian national interest.* It cannot be in accordance with the interest of the safety of Russia that Germany should plant itself upon the shores of the Black Sea, or that it should overrun the Balkan States and subjugate the Slavonic peoples of south eastern Europe, That [sic] would be contrary to the historic life-interests of Russia. (Churchill, 1939)

Despite his confusion over why Russia would cooperate with fascists that hated it and against who they had once railed, Churchill hill posited that Russia would eventually oppose the Nazis if they invaded the Balkans or the Slavic areas adjoining the Black Sea—the area Ukraine inhabits. Indeed, key parts of Ukraine, such as Kiev, have been ruled by the Russians since the 17th century—a time
when the territory now known as the United States of America was still mostly wilderness and largely the domain of Native Americans (Nygren, 2008). Indeed, the “historic life-interests of Russia” could have easily predicted reprisals from Russia for the Euromaidan Revolution that overthrew the Russian supported Yanukovych government and the highly unpopular (in Russia, that is) US and Western European interventions in the Balkans—interventions the Russian officials such as General Valeri Gerasimov who now lead the efforts against Ukraine have criticized (Gerasimov, 2016b; Cordesman, 2017).

As discussed above, many controversial Russian actions can be viewed as Russia pushing back against what it sees as efforts by the United States and its European allies to foment revolution across the world. Ukraine—having fought Russian forces to a stalemate—is a country now largely on the defensive against the hybrid war being fought against it, and it will remain on the defensive as long as Russia views it in its interests to attack it and support the war in eastern Ukraine. Russia is much more powerful on every level, and its seat on the UN security council means that it can and will veto any attempts to use the UN against its aggressive actions. Russia also supplies gas and oil to Europe through pipelines built during the Soviet Union and newer projects like North Stream I and II—the second pipeline being built despite European sanctions (Klikushin, 2018). Indeed, with a popular former German prime minister (Gerhard Schröder) lobbying on behalf of the Russian energy industry and sitting on its boards, it is unlikely that sanctions against Russia will ever be strong enough to economically dissuade it from aggression in Ukraine (Noack, 2017). In fact, Germany already receives 75% of its gas from Russia and faces internal opposition to efforts to confront Russia’s brazen misbehavior—whether invading Ukraine or using chemical weapon to assassinate a former spy as a warning to
other potential defectors (Chambers 2018; Keating 2018). Indeed, countries like Italy openly question whether sanction should exist at all—no doubt influenced by the continuing political influence of populist Silvio Berlusconi (Emmott & Baczynska, 2016).

Ukraine on the other hand is one of the poorest countries in Europe and, despite one of the largest militaries in Europe, is ill-equipped. Although secondary parties like the US, Poland and the Baltic States have supported Ukraine with training and equipment, the military gap between Russia and Ukraine remains large and likely insurmountable—Russia will always have nuclear weapons and Ukraine will likely never have them in it again. Given this power asymmetry and the prospect of a war without end—what can Ukraine do? One intervention—in concert with other interventions—is to reduce the violence on the line of control in eastern Ukraine. As the OSCE recently noted, the violence there has the potential to spin out of control into a high intensity war where Russia abandons all pretext of not being a direct combatant with Ukraine (Shalal, 2018). At the very least, Ukraine can reduce civilian casualties—something that risks only further dividing Ukrainian society. For this, this section argues using Dr. Gary Slutkin’s approach of treating violence as a contagious disease. Infectious diseases have three major characteristics: clustering, spread, and transmission (Slutkin, 2013). Clustering is fairly self-explanatory—violence is often close in time and distance to other violence. Spread means that violence propagates in a non-linear fashion meaning that strict causation is hard to determine and its onset is due to multiple factors. It can occur in waves—like the plague and then die out. Finally, it is transmitted from person to person. Other researchers, such as Yale’s Dr. Andrew Papachristos, have shown how violence and criminality is embedded within social networks and therefore can be both predicted
and possibly prevented—such as through the Chicago Police Department program known jokingly as “hug-a-thug” in the department (Christensen, 2014).

Although other application areas—such as Chicago gang violence—are quite different from a ceasefire line, an OSCE map shows that civilian deaths are quite similar to the patterns of disease outbreaks and Chicago gun violence (Fig. 4). Indeed, OSCE (2017) has found the kind of correlations one would expect with the clustering, spreading, and transmission of a disease-like violence dynamic: “there is a correlation between ceasefire violations and corroborated cases of civilian casualties caused by shelling and SALW and that increased intensity of fighting contributes to an increase in the number of civilian casualties” (p. 10). Cure violence—the NGO Slutkin uses to implement his model—recommends seven steps, which can be modified and applied to eastern Ukraine and should be implemented on both side sides as much as possible:

1. Assess the violence problem along the line of control/ceasefire line
2. Engage leaders of communities
3. Identify appropriate community partners
4. Identify appropriate hospital response partners
5. Re-examine the data
6. Hire and train credible workers
7. Implement program with technical assistance (Cure Violence, 2018)
Figure 4. Cholera Epidemic and Violence in Chicago (Slutkin, 2013) Compared with an OSCE Map of Civilian Casualties in Eastern Ukraine (OSCE, 2017).

Although separatists who live in the community can be reached through community leaders, those in the Ukrainian and Russian military may be harder to intervene with, because they must act on orders or face discipline. Indeed, most of those engaging in the
violence in this situation are under some sort of chain of command. Thus, commanders with discretion to retaliate or not to ceasefire violations may be a key target in this intervention. There is evidence this may work—President Poroshenko has repeatedly ordered Ukrainian Soldiers to only fire when attacked—something that has helped decrease ceasefire violations from thousand to tens per day (Unian, 2015). In addition, a PeaceTXT-like intervention where messages are delivered to residents in the communities along the line of control that warn of active combat and shame combatants on both sides for killing civilians with their barrages. Messages like: “You just killed Svetlana, a four year old child,” “stop firing, you are hitting civilians” or “violence is killing the people you claim to protect.” PeaceTXT uses the idea that these messages and interventions can act as violence interrupters and are used in many different contexts—from Kenya to prevent election violence to Chicago to prevent gang violence (Ushahidi, 2011). Other methods that mobile texts, like WhatsApp, Viber, Telegram and Facebook messenger could all facilitate this messaging and each of these is widely used in Ukraine.

Using the seven steps advocated by Cure Violence and the PeaceTXT messaging model, violence along the Line of Control in eastern Ukraine could likely be lowered. Ukraine cannot defeat Russia militarily, and Russia is unlikely to view a withdrawal from Ukraine in its national interest in the near future. Further, Russia is likely to continue to assault Ukraine using Information and Political Warfare in line with the Gerasimov’s approach, and although interventions should be made to combat this, interventions can also be made to reduce civilian deaths to close to zero as possible if a ceasefire cannot be fully implemented. Thus, even if Minsk II remains a failure, interventions using Dr. Slutkin and Cure Violence’s methods can help reduce the violence along the line of country.
Chapter VI.
Conclusions

Gerasimov’s approach to hybrid war is a key insight into how Russia has and will conduct the war in Ukraine—although it is not the only the influence and is part of larger of evolution of Russian approaches to the cyber and information domains. Due to General Gerasimov’s position as Chief of the General Staff of the Armed Forces of the Russian Federation and First Deputy Minister of Defense of the Russian Federation, his closeness to the highly influential Defense Minister Sergei Shoigu and his willingness to argue for the modernization of the Russian military in a way that uses advanced low cost and high impact hybrid war techniques, it is likely that the general’s influence will only increase. Despite setbacks in the war in Eastern Ukraine, the unequivocal success of the operation in Crimea (in terms of a military operation, at least), the highly successful Guccifer 2.0 Clinton email operation, and evidence of other Russian international information warfare efforts to “polarize democratic societies and pit communities within those societies against each other” indicate Russia will only continue to rely on both on Gerasimov directed and influenced operations as well as those efforts of a similar character—whether of a civilian or military intelligence character (Garcia & Torres, 2018).

Even if Gerasimnov’s approach to hybrid warfare is not his own invention, the result of the collective reflection of many in the Russian military or simply him parroting Russian military policy, he remains one of the clearest and concise articulation of the hybrid methods of war being employed in Ukraine and across the world. The evidence from the language of his articles and speeches, though, indicates someone who actively advocating for the Russian military to adopt approaches that compete with and in many
way mirror the low cost, high impact color revolution style military campaigns he imagines the West—particularly the US—uses to great effect.

The Putin guided Russian vision for a multipolar world with spheres of influence where Russia is an important international player is facilitated through these color revolution-like campaigns and are a way to keep its former colonial possessions—like Ukraine in check and under its influence. Modern Russian information warfare combines the parallel and intertwined developments of the Russian economic and political system. Likewise, Russian Cyberwarfare leverages these developments as well. Gerasimov’s approach is the logical extension of these developments—utilizing the assets Russia has developed to gain a military advantage. Both Gerasimov’s vision of modern warfare and the information and cyber warfare capabilities that grew from chaotic and dark economic transition from communism to a market economy are a dark mirror of Western institutions and the attempt to spread liberal democracy and capitalism across the globe.

Ukraine’s best hope in the war in Eastern Ukraine is to descale it as much as possible to ensure the conflict does not escalate and serve as a pretext for the final stages of Gerasimov’s 2013 vision of hybrid war a peacekeeping occupation or simple full scale invasion by using the overwhelming force of the Russian military. While waiting, Ukraine can do everything possible to save the lives non-combatants and its own soldiers while it upgrades its military with the support of the US and Western European allies. Ukraine will never have the capability to counter Russia’s nuclear superiority and purported willingness to use them without having the unequivocal protection of the US’s nuclear arsenal through NATO. Instability in Russia, a souring of public opinion on the war, conflict with another powerful neighbor, a drastic change in political leadership or even simply the death of Putin could all change Russia’s calculus and open the door for
peace. Ukraine has much work to be done internally and can use this opportunity to reform the country and decrease its reliance on Russia and thus its ability to force it to act in one way or another.

This area remains full of opportunities for future research. For instance, there is a clear link of Russian hybrid warfare to modern civilian social media marketing, but this disciplinary lens is rarely applied in-depth due to its focus on business and economic dynamics. Likewise, a biographical sketch of General Gerasimov from those who worked with him and in his own words would help many understand this general who is a key part of the powerful resurgence of the Russian military on the international stage.
References


http://thetechnofreaks.com/2012/05/31/flame-malware-everything-you-need-to-know-about-the-worlds-most-dangerous-malware/


https://www.wsj.com/articles/SB10001424052702304709904579406310892324006


http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx


http://all.net/books/Dissertation.pdf


usa/russia-meddling-in-mexican-election-white-house-aide-mcmaster-
idUSKBN1EW0UD


Markov et al. (2016, June 5). *Has Russia been planning this annexation of Crimea for years now along with an annexation of heavily pro Russian areas in Eastern Ukraine?* Retrieved from https://www.quora.com/Has-Russia-been-planning-this-annexation-of-Crimea-for-years-now-along-with-an-annexation-of-heavily-pro-Russian-areas-in-Eastern-Ukraine


http://www.cidcm.umd.edu/mar/assessment.asp?groupId=37204


Toal, G. (2017). *Near Abroad: Putin, the West and the Contest Over Ukraine and the Caucasus.* Oxford University Press.


http://blog.twitter.com/2012/07/twitter-transparency-report.html


