Russian Information Operations and the Rise of the Global Internet

Teyloure Ring

A thesis submitted in partial fulfillment of the requirements for the degree of
Master of Arts in International Studies: Russia, East Europe, & Central Asia

University of Washington
2015

Committee
Scott Radnitz
Volodymyr Lysenko

Program Authorized to Offer Degree:
Jackson School of International Studies

Teyloure Ring

University of Washington

Abstract

Russian Information Operations and the Rise of the Global Internet

Teyloure Ring

Chair of the Supervisory Committee:

Professor Scott Radnitz

Jackson School of International Studies

For centuries the pursuit of competing political objectives has led to military conflict. Prussian military theorist Major-General Carl von Clausewitz wrote, "War is thus an act of force to compel our enemy to do our will."[1] History has shown that the ability to affect an adversary's information and information systems augments the effects of kinetic operations. Therefore, command and control and communication nodes are frequently early targets during times of war. Disrupting the flow of information is essential for militaries seeking an advantage over an adversary. Attacks on communication centers have been documented in numerous conflicts including the American Civil War, World War I, and World War II.[2]

Information operations were a supporting element of military strategy, secondary to kinetic operations until Operation Desert Storm. The use of information technologies to exploit

an information differential in Iraq contributed to the swift success of coalition forces. Operation Desert Storm marked the first time information technologies were used to create an asymmetric advantage in modern warfare.[3] Military strategists around the globe began exploring the value of these technologies in information operations. Understanding how these new technologies are used to create an asymmetric advantage in wartime is critical for developing effective countermeasures. This piece addresses the adoption of information technologies and cyber tools in Russian information operations in Chechnya, Estonia, Georgia, and Ukraine.

1. Introduction

Russian information operations in Ukraine were in place before the Third Eastern Partnership Summit in Vilnius on 28-29 November 2013. They supported Russian efforts during the annexation of Crimea in March 2014 and remain underway. The successful integration of cyber tools in the information campaign against Ukraine contributed to the swift consolidation of Russian power in Crimea and is central to the vitality of current operations. Like the campaigns against Chechnya and Georgia, the information operations underway in Ukraine use deception, psychological operations, active measures, and reflexive control. The campaign against Ukraine illustrates the value of cyber tools in amplifying traditional information operation effects.

The NATO Strategic Communications Center of Excellence (NATO StratCom COE) explains: "During the crisis in Ukraine, we have witnessed the application of a new type of warfare where dominance in the information field and hybrid, asymmetric warfare are the key element…Applying the elements of the new type of warfare, victory can be ensured without open military conflict and deployment of large amounts of military power to the conflict area."[4] The activities in Ukraine represent the convergence of evolving information operations theory with decades of Soviet and then Russian military thought. Through a comprehensive exploratory case study, this piece seeks to understand the growing role of cyber tools and the Internet in Russian information operations. The Russian influence campaigns employed against Chechnya, Estonia, Georgia, and Ukraine were selected to illustrate the increase in use over time.

2. Literature Review

2.1 Information Operations

The U.S. Joint Chiefs of Staff define information operations as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation, to influence, disrupt, corrupt, or usurp the decision of adversaries and potential adversaries while protecting our own."[5] Operation Desert Storm set a precedent for information operations in modern warfare. The use of information technologies was a significant force multiplier during the conflict. Col Edward Mann, United States Air Force explains the importance of information technologies in modern warfare in his piece *Desert Storm: The First Information War?*. Col Mann writes:

> Rapidly gaining and exploiting information dominance was clearly a key goal of the Desert Storm air campaign plan. The first Iraqi targets attacked were air defense, leadership (including command, control, communications, and intelligence), and electrical grids, all of which had the highest priority because of their impact on the Iraqis' flow of information. The integrated air defense command and control system, known as Kari (Iraq spelled backwards in French), provided tracking and targeting information for Iraqi fighter and surface-to-air missile (SAM) engagements of coalition aircraft. Breaking down this flow of information would fragment the enemy's air defense effort, forcing his SAMs into autonomous mode and leaving his interceptors virtually helpless. This situation allowed coalition aircraft to exploit Iraqi airspace at will. Leadership targets provided linkages between the highly centralized decision-making elements (principally Saddam) and both the Iraqi population and the fielded military forces. Disrupting these systems would upset and discredit the regime, while simultaneously reducing its capability to control military forces. Without electrical power, communications would be reduced to verbal and handwritten messages conveyed by courier. Thus, a successful attack against the Iraqi power grids would disrupt nearly every kind of information flow within the nation. Plans called for maintaining pressure on Iraqi "information nodes" throughout the war to help create an exploitable "information differential."[6]

Operation Desert Storm exemplified the value of combining information operations with cyber and electronic warfare. In 1991, Lieutenant-General S. Bogdanov of the Soviet Armed Forces General Staff Center for Operations and Strategic Studies stated, "Iraq lost the war before it even began. This was a war of intelligence, electronic warfare, command and control, and

counterintelligence. Iraqi troops were blinded and deafened…Modern war can be won by informatika and that is now vital for both the United States and the USSR."[7]

Russian military theorists were acutely aware of the emergence of information technologies in Operation Desert Storm as an essential component of modern warfare. It was clear to experts that "these technologies must be embedded into new military equipment, from sensors and radars to jet fighters and cruise missiles. However, Russia was also concerned about the impact of information technologies on the brain and consequently morale."[8] According to literature regarding Russian military reform in the 1990s, "these technologies included the rapid distribution of information via the mass media and Internet."[9]

Russian attention to information technologies and their value to psychological operations is a continuation of Soviet interest. Beginning in 1942, the Military Institute of Foreign Languages offered *spetspropaganda* (special propaganda) theory as a subject. After institutional reorganization it is now a part of the Military Information and Foreign Languages Department of the Military University of the Ministry of Defense of the Russian Federation curriculum.[10] It is important to note there are several differences between the Russian and Western definitions of information warfare. Russian theorists view information warfare "as influencing the consciousness of the masses as part of the rivalry between the different civilizational systems adopted by different countries in the information space by use of special means to control information resources as 'information weapons.'".[11] Compared to Western views, the Russian approach combines "the military and non-military order and the technological (cyberspace) and social order (information space) by definition, and make direct references to 'Cold War' and 'psychological warfare' between the East and the West."[12]

The language and propaganda use suggesting a "Clash of Civilizations" between Orthodox Eurasia and the West was of significant value in Russian information operations in Ukraine and Georgia.[13] The Russian government used this narrative to justify its actions. Cyber tools were widely employed in the promotion of this narrative. "Control of narratives is seen as a more powerful tool than setting the media agenda, because recipients of the information reject those stories that contradict their 'base narrative' or 'strategic narrative.' Narrative control means control over the process of interpreting information."[14] State-sponsored narratives are prevalent in conflicts around the world, their application in Russian information operations is addressed in later chapters.

The information campaign against Ukraine highlights the evolution of Russian methods since the 2008 Russian-Georgian War. The 2008 conflict was the first in which a wide scale cyber-attack acted as a force multiplier for a kinetic invasion. Tactics used in Ukraine were tested and perfected first in Chechnya then Estonia and Georgia. The value of cyber tools and use of information communication technologies is exemplified by the two Chechen wars: while there was no "change in the location or practice of war, their narratives and thematic frameworks were significantly different and this affected the international position of the two parties involved."[15] Understanding the confluence of traditional information operations tactics and cyber tools is essential for developing effective countermeasures.

2.2 Information Operations and the Internet

Russian information operations draw heavily on traditional Soviet methods based on a combination of active measures and reflexive control. The rise of the global Internet and

information and communication technologies has taken the struggle for information dominance to cyberspace.

The Committee for State Security (KGB) was responsible for managing active measures, a term used to refer "to deceptive operations conducted in support of Soviet foreign policy."[16] Active measures included:

- **Disinformation and forgery**: Deliberate attempts to deceive public or government opinion by forging facts or documents
- **Front groups and friendship societies**: Coordinated activities in non-government, non-political organizations engaged in promoting certain goals
- **Non-ruling Communist and Leftist parties**: Liaison with the parties to engage them in specific political action or propaganda campaigns on behalf of the [Soviet Union]
- **Political influence operations**: Disguised KGB agents take active roles in the respective nation's government, political, press, business or academic affairs
- **Russian Orthodox Church**: Integrated financially as well as structurally into the Soviet foreign propaganda apparatus to support the implementation of active measures[17]

Soviet and Russian literature explains active measures as necessary to counter information aggression from the West and other enemies of the Soviet and successive Russian state.[18]

Another central component of Russian information operations is reflexive control. "Reflexive control is defined as a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[19] Russian reflexive control plans include discrediting governments and institutions as evidenced in Chechnya, Georgia, and Ukraine.

General Anatoliy Nogovitsyn, Deputy Chief of General Staff of the Armed Forces of the Russian Federation, Colonel General defines information warfare as:

> Conflict among states in the information space with the objective of inflicting damage on information systems, processes, and resources and on critically important structures, undermining the political and social systems, and massively

> brainwashing troops and the population with the objective of destabilizing the enemy society and the state as a whole.[20]

"With regard to the latter information-psychological effect, Nogovitsyn added that the human mind is the objective of this aspect of warfare against which different information technologies can be directed."[21] Russian active measure and reflexive control techniques have evolved drastically as a result of the rise of the global Internet and information communication technologies. Information can travel cheaper, faster and to a wider audience in cyberspace than ever before.

Cyber tools can provide an asymmetric advantage for actors seeking to gain information dominance on the Internet. Cyber tools are used to collect intelligence, publish information or disinformation, engage in dialogue with various groups and individuals, and coordinate action. However, they can also be used for more nefarious purposes, and while cyber tools are confined to virtual reality, their use has real world effects. Traditional warfare targets such as air traffic control systems, nuclear reactors, SCADA (Supervisory Control and Data Acquisition) systems, power grids, telecommunications infrastructure, news stations, banking and finance, oil and gas distribution networks, water supplies, and emergency and government services are susceptible to cyber-attacks, as evidenced in Estonia, Georgia, and Ukraine.

The Russian strategy employs hacking techniques such as web hacks, computer break-ins, computer viruses, computer worms, and denial of service attacks. These tools are particularly helpful for launching disinformation campaigns, discrediting governments and institutions, and promoting a state supported narrative necessary for the psychological conditioning central to reflexive control.

For example, a denial of service attack may be initiated during a campaign attempting to discredit a government or institution. A denial of service (DoS) attack is when "an attacker attempts to prevent legitimate users from accessing information or services."[22]According to the

United States Computer Emergency Readiness Team, the most common type of DoS attack results when an attacker floods a network. When a computer user enters a website URL into a browser, it simultaneously sends a request to the site's computer server to view the website. "The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process" those of legitimate users.[23]

A denial of service (DoS) attack becomes a distributed denial of service (DDoS) attack when the attacker uses multiple computers to launch the attack. This can be done using a botnet. A botnet is a network of computers that are controlled from a single source. The computers are typically infected with malicious software that enables an attacker to mobilize the botnet to for example, send spam, infect other machines with malware, or execute a distributed denial of service attack. During the 2008 Russian-Georgian War, the Euromaidan protests, the annexation of Crimea, and aggression in the eastern part of Ukraine, DDoS attacks frequently targeted Georgian and Ukrainian government websites. While a DoS attack renders a site inaccessible, other hacking techniques may be employed in attempt to discredit a government or institutions. The defacement of Estonian, Georgian, and Ukrainian presidential and parliamentary websites is addressed in later chapters. The under-researched rise of pro-Russian Internet trolling is discussed as well.

3. Methodology

Understanding the integration of cyber tools in Russian information operations requires detailed evaluation of the influence campaigns in which they occurred. The most appropriate research methodology for this type of analysis is a comprehensive exploratory case study. I used this approach to assess the role of information communication technologies in each case.

In my data collection process, I reviewed English and Russian primary and secondary sources covering Russian information operations in Chechnya, Estonia, Georgia, and Ukraine. Russian policy doctrines, publications by military and geopolitical strategists, and screenshots of cyber activity such as attack instructions or website defacements serve as primary sources.[24] Secondary data sources include published interviews of participants in the influence campaigns and works by military and cybersecurity experts and various researchers.

I began my research on Russia's influence campaign in Ukraine before the annexation of Crimea. With little more than a year having elapsed since the annexation of Crimea, there are few publications in scholarly journals addressing Russia's actions and the continued violence in the eastern part of Ukraine. As a result, a majority of the sources referenced in the Ukraine case study is from Internet-based information outlets.

Through the combined use of numerous printed and Internet-based sources, I was able to triangulate data between many sources thereby increasing the validity of my findings. These sources provided enough information to conduct an exploratory case study of Russian influence campaigns. Through the various cases, I was able to evaluate the integration and increasing use of cyber tools in Russian information operations.

4. Russian Information Operations Reform and Chechnya

Russian military strategists first tested information operations theories during the First Chechen War (1994-1996). While Russian forces made gains militarily, Chechnya's Ministry of Information was winning the battle for public opinion.[25] During the conflict, Federal forces rarely engaged with the media, a likely continuation of the Soviet aversion for the press. This sharply contrasted with the Chechen engagement with Russian journalists and media. Russian journalists

enjoyed free travel to Chechnya where they would interview the local population and Chechen forces. Sources report that the Russian military's organic assets "did less than 5 percent of the reporting in January 1995 of the news coming from Chechnya…As a result, Russia's citizens only saw what was important from the Chechen point of view on the evening news."[26] Chechen commanders also used mobile television transmitters to capture atrocities committed by Federal forces. Information communication technologies were essential for the rapid dissemination of the one-sided, pro-Chechen materials through traditional channels and the Internet.

Russian information operations during the conflict were a dismal failure. While Russian military strategists reformed their theories, the crisis in Yugoslavia waged on. Ending shortly before the Second Chechen War began, the Kosovo War galvanized the importance of the global Internet for Russian strategists. The Yugoslav conflict "has been characterized as the first war on the Internet."[27] The Internet was a theater for government and nongovernment actors seeking to "disseminate information, spread propaganda, demonize opponents, and solicit support for their positions. Hackers used it to voice their objections to both Yugoslav and NATO aggression by disrupting service on government computers and taking over their websites."[28] The Internet directly influenced the political discourse surrounding the war and had a clear impact on military decisions. "While NATO targeted Serb media outlets carrying Milosevic's propaganda, it intentionally did not bomb Internet service providers or shut down the satellite links brining the Internet to Yugoslavia."[29]

Russian military strategists noted the Western response. The precursors to the conflict in Kosovo had an uncomfortable amount of similarities for the Russians as tensions in Chechnya continued to rise. Like Kosovo, Chechnya faced increasing ethnic violence and demands for independence. The Kosovo War highlighted the importance of information technologies in modern

conflicts. The West confirmed Russian views of the strategic value of the Internet when in April 1999, the *Washington Post* wrote that "according to U.S. and British officials, NATO governments controlled all four Internet access providers in Yugoslavia and kept them open for the purpose of spreading disinformation and propaganda."[30] This affected the organization of Russian information operations for the Second Chechen War.

When the Second Chechen War began in August 1999, Russian authorities severely restricted independent media to ensure the protection of the state-supported narrative.

> Russia's strategy was to 'reprogram the mass consciousness' by introducing a number of information-propaganda clichés into it. These included the development of 'models' [such as] the terrorist and aggressor model; the 'new war' model (this time the army is ready); and the 'Free Chechen' model (convincing Russian society that Chechens were simply waiting for the Russian armed forces to liberate them)[31]

Strict controls on the media were essential for the Russian strategy. However, Chechens were able to bypass the Russian-imposed information blockade via the Internet.

Chechens skillfully used the Internet to raise funds (amino.com), unite the Chechen diaspora, and spread material about their position and the atrocities committed against the Chechen population. Lieutenant Colonel Timothy L. Thomas, U.S. Army, explains that the Chechens also used the Internet "to rally Islamic faithfuls worldwide against the Israelis in their conflict with the Palestinians, serving to unite a religious sector of the world population."[32] The increase in online activity did not go unnoticed. "Russia soon moved from what contemporary cyber warfare theory terms computer network exploitation (cyber espionage) to computer network attack during the latter days of the second Chechen War…in an effort to control information flow. Chechen targets included kavkaz.org and chechinpress.com (now defunct) and were of sufficient size to knock both sites off the air."[33] The rise of information communication technologies and the Internet solidified the importance of securing dominance in the information domain.

When Russian President Vladimir Putin ascended to power in 2000 he emphasized the importance of a strong cybersecurity posture and information operations. The 2000 Information Security Doctrine identifies Russia's threats on the information front.[34] "The decade after the 2000 Information Security Doctrine saw an explosion of information operations writing by Russian military officers and defense oriented academics."[35] For example, Russia celebrated the "first ever Electronic Warfare Specialist Day on 15 April 2000."[36] Twenty-first century Russian information operations strategy utilizes the effects of cyber tools. In 2006, Russian State Duma Deputy and Member of its Security Committee Nikolai Kuryanovich said, "In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers. This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces."[37]

The 2007 cyber-attack on Estonia will be examined in the next section as a trial-run for the cyber component of the 2008 Russian-Georgian War. Russian information operations strategies pertaining to the information-psychological activities and morale-psychological condition of Russian soldiers and related morale-psychological problems while important, are beyond the scope of this paper.

5. Russian Information Operations and Estonia

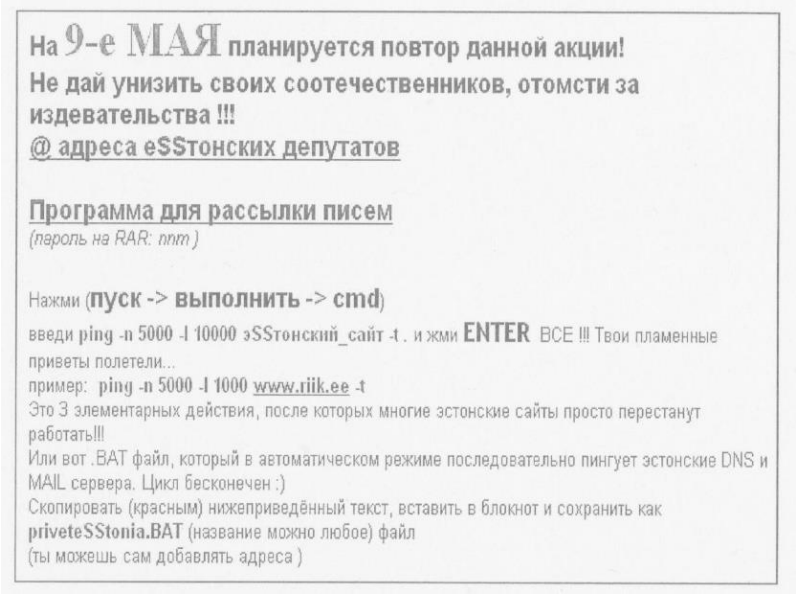
On the night of 26 April 2007, the Estonian government relocated the Bronze Soldier, a monument commemorating the Soviet liberation of Estonia during World War II. The statue and the Red Army soldiers buried beneath it were moved from Tõnismägi Park in the city center to Tallinn Military Cemetery on the outskirts of the city. While "many Estonians see the war monument as a symbol of the Soviet occupying force and the annexation of the Baltic states," its

removal was perceived by many Russians as an insult to the veterans who fought to liberate the Baltics from Nazi rule.[38] The monument's relocation was protested by Russian government officials, officials of some other former Soviet countries, the Patriarch of Moscow, and some citizens in Estonia and Russia. The next day on 27 April 2007, a massive 22-day coordinated cyber-attack was launched against Estonia. Many have characterized it as Europe's first information war. The hallmarks of the attack as well as Moscow's subsequent indirect economic sanctions, pressure on the Estonian government to revise legislation regarding the treatment of Russian minorities, as well as labeling the Estonian government "a Fascist or pro-Fascist regime suggests Moscow's hand behind the attack."[39]

"Estonia, although small, is a remarkably Web-dependent country, with widespread Internet access, digital identity cards, an 80-percent usage rate for online banking [in 2007], electronic tax collection, and remote medical monitoring."[40] The sustained cyber-attack "targeted Estonia's essential electronic infrastructure, banks, telecommunications, media outlets, and name servers, thus threatening the entire nation's security."[41] The Estonian Defense Minister Jaak Aviksoo said "It is true to say that the aim of these attackers was to destabilize Estonian society, creating anxiety among people that nothing is functioning, the services are not operable, [and] this was clearly psychological terror in a way."[42] The attack supported traditional information operations goals.

The cyber-attack consisted of two waves. The first wave used simple cyber tools, Russian websites encouraged people to engage in attacks, provided software downloads with easy-to-follow instructions and targeting information. The Estonian Government Briefing Room, the Estonian Ministry of Defense and other government sites were targeted.

The second wave began in the late evening of 8 May and early morning of 9 May. More sophisticated techniques were employed, large botnets were used to simultaneously launch DDoS attacks on the websites of the Estonian Parliament, the country's two largest banks, six of the largest news organizations and telephone exchanges. The start date of the second wave coincides with the politically important Victory Day in Russia, a celebration of victory over Nazi Germany. Online instructions (Figure 1) identified 9 May as the start date for attacks.[43] However, "the big attack wave anticipated for May 9th started shortly after 11PM in Estonia on May 8th… suggesting that these attackers were on Moscow time."[44]


На 9-е МАЯ планируется повтор данной акции!
Не дай унизить своих соотечественников, отомсти за издевательства !!!
@ адреса eSStонских депутатов

Программа для рассылки писем
(пароль на RAR: nnm)

Нажми (пуск -> выполнить -> cmd)
введи ping -n 5000 -l 10000 эSStонский_сайт -t . и жми ENTER ВСЕ !!! Твои пламенные приветы полетели...
пример: ping -n 5000 -l 1000 www.riik.ee -t
Это 3 элементарных действия, после которых многие эстонские сайты просто перестанут работать!!!
Или вот .BAT файл, который в автоматическом режиме последовательно пингует эстонские DNS и MAIL сервера. Цикл бесконечен :)
Скопировать (красным) нижеприведённый текст, вставить в блокнот и сохранить как priveteSStonia.BAT (название можно любое) файл
(ты можешь сам добавлять адреса)

Figure 1

Throughout the cyber-attack on Estonia, "the malicious traffic often contained clear indications of political motivation and a clear indication of Russian language background. For example, malformed queries directed at a government website included phrases like "ANSIP_PIDOR=FASCIST" (Mr. Ansip was the Estonian Prime Minister at the time). Dozens of variants were used, often containing profanities."[45]

The organization of the cyber-attack on Estonia fits cybersecurity expert Jeffrey Carr's three-tier model of command and control. Carr explains:

> It's understandable to want to find a telltale piece of evidence that conclusively links the Kremlin with the actions of its hackers. However, it's important to realize that in the anonymous workings of the Internet, such a goal is not only naïve, but it

> also doesn't accurately represent the relationships that have been built over the years between Russian politicians and organized youth associations.[46]

Carr's three-tiered model "established command and control by the Kremlin through Nashi (Youth Democratic Anti-Fascist Movement 'Ours') and other groups whose membership include hackers, resulting in an organized yet open call for unaffiliated hackers to join in. Russian organized crime provides a protected platform from which these attacks can then be planned and launched. And all of this occurs while providing a cover of plausible deniability to the state."[47] Carr's idea was reinforced when Nashi activist Konstantin Goloskolov "confirmed that the group was behind the cyber-attack against Estonia of spring 2007" in an interview with the *Financial Times*.[48] Carr's model can be applied to the cyber components of the 2008 Russian-Georgian War and 2014 annexation of Crimea.

Dr. Stephen Blank explains that in addition to the cyber-attack, "Moscow organized violent demonstrations in Tallinn among the Russian diaspora there and among its homegrown youth organization in Russia, Nashi, and in Moscow against the Estonian embassy."[49] Estonian authorities believe the violence incited by Estonia's Russian diaspora was meant to serve as "as a pretext by Moscow to intervene and launch a kind of insurgency directed against Estonia that could have justified either direct Russian support for the insurgents or some form of direct, even military, intervention from Russia."[50] Estonian authorities also "recorded the presence of Russian Special Forces in civilian clothes (it is not clear which of the many different kinds of the Russian Special Forces they meant) at the demonstrations."[51] This tactic was used in Crimea in 2005 during anti-NATO protests and again during the 2014 annexation of Crimea and aggression in the eastern part of Ukraine.

The Estonian case illustrates the development of a "longstanding Russian strategy for asymmetric war or conflict."[52] Dr. Stephen Blank explains, "The elements of this strategy are cyber

war, economic sanctions, a domestic and international public information campaign against Estonia, the manipulation of youth organizations or gangs, and ongoing Russian efforts to penetrate key sectors of the Estonian economy and subvert politicians."[53] Dr. Blank further explains, that "connections with the energy industry or through intelligence penetration, and the links between Russian organized crime and Baltic elites in general" support the Russian strategy.[54] However it is important to note that "this strategy and any or all of its elements obviously need not be confined to the Baltics or Eastern Europe or only to Russian use."[55]

The 2014 annexation of Crimea and events in the eastern part of Ukraine illustrate the continued evolution and success of Russian strategy. The next section addresses the cyber component of the 2008 Russian-Georgian War. Russian Deputy Premier and former Defense Minister Sergei Ivanov foreshadowed the use of cyber tools in information operations when he said:

> The development of information technology has resulted in information itself turning into a certain kind of weapon. It is a weapon that allows us to carry out would-be military actions in practically any theater of war and most importantly, without using military power. That is why we have to take all the necessary steps to develop, improve, and, if necessary—and it already seems to be necessary—develop new multi-purpose automatic control systems, so that in the future we do not find ourselves left with nothing.[56]

His statements proved true in the Russian-Georgian War and the events in Ukraine.

6. Information Operations and Georgia

In mid-July 2008, weeks before the Russian-Georgian War began, the website of President Mikhail Saakashvili was the target of a distributed denial of service attack. The website was also defaced with a moving slideshow comparing Saakashvili to Hitler. The preemptive attack on the President's website supported Russian information operations by limiting the Georgian government's ability to communicate with its citizenry and contributing to the state-supported anti-

fascist narrative. On 8 August 2008, Russian troops invaded Georgia and at the same time traditional warfare targets came under cyber-attack in the country. The Russian-Georgian War is considered by many to be the first time when a coordinated cyber-attack was used as a force multiplier for a kinetic invasion. There are many similarities between the cyber-attacks on Estonia, Georgia and Ukraine.

On the first day of the war, the cyber-attack targeted local news agencies and websites in the small town of Gori, where the ground invasion began. Other targets included "the websites of the president of Georgia, the Georgian Parliament, the ministries of defense and foreign affairs, the National Bank of Georgia" and online news agencies.[57] The start times of the cyber-attack and the kinetic invasion suggest that "organizers of the cyber-attack had advance notice of Russian military intentions, and they were tipped off about the timing of the Russian military operations while these operations were being carried out."[58] Furthermore, "when the cyber-attacks began, they did not involve any reconnaissance or mapping stage, but jumped directly to the sort of packets that were best suited for jamming the websites under attack."[59] The computer network exploitation and cyber reconnaissance efforts preceding the attack were consistent with the methods employed against Estonia.

As in the attack against Estonia, the cyber-attack against Georgia used DDoS, SQL injections and website defacements. And like the attack on Estonia, Russian language websites and forums were used to recruit civilians to participate. The intimate knowledge of Russian military operations the organizers of the attack had, in combination with the use of Russian language forums and civilians, suggests the use of Jeffrey Carr's three-tiered command and control model whereby the Kremlin creates plausible deniability in the attacks by using a mediator to recruit compliant civilian hackers.

To further support Carr's model, the forums used to recruit hackers have been linked to illegal activities associated with organized crime syndicates. For example, stopgeorgia.ru and Xakep.ru (the Russian term for hacker), were websites that recruited civilian hackers. The platform "stopgeorgia.ru was set up within hours of the Russian Armed Forces invading South Ossetia... lists of target websites were featured and visitors were encouraged to download a free software program, which allowed them to participate instantly in massive DDoS attacks."[60] A study conducted by the Swedish National Defense University revealed that "stopgeorgia.ru is related to different criminal activities, such as forged passports and stolen credit cards, i.e. activities that normally should be prosecuted by the authorities; however, the Russian authorities have remained remarkably passive in prosecuting the person in this particular case."[61]

An open-source intelligence investigation into the Russian government involvement in the cyber-attacks against the Georgian government, Project Gray Goose, revealed that the stopgeorgia.ru IP address 75.126.142.110 "resolves to a small Russian company called SteadyHost."[62] According to the Swedish Defense Research Agency, "SteadyHost is believed to have its offices in the same building as a Ministry of Defense institute, the Russian Center for Research of Military Strength in Foreign Countries. The Main Intelligence Directorate's headquarters is also situated on the same street."[63]

Methods similar to those employed in Estonia were used to target government websites, financial institutions, business associations, educational institutions, hacking forums and energy sources. According to the U.S. Cyber Consequences Unit, "The targets for attack were nearly all ones that would produce benefits for the Russian military. The one target for cyber-attack that was somewhat unusual from a military standpoint was a website for renting diesel-powered electric generators." [64] However, this target likely buttressed the effects of physical strikes that targeted

the Georgian power grid. “More strikingly still, the news media and communications facilities, which would ordinarily have been attacked by missiles or bombs during the first phase of an invasion were spared physical destruction, presumably because they were being effectively shut down by cyber-attacks.”[65] By targeting news agencies and government websites, the cyber-attacks effectively reduced the Georgian government’s ability to communicate with the public during wartime; thereby accomplishing the Russian information operations objectives of severing communication nodes and discrediting the regime. “The inability of Georgia to keep these websites up and running was instantly damaging to national morale,” and “these attacks served to delay any international response.”[66]

Like the information campaign against Estonia, the cyber-attacks against Georgia labeled the government as fascist regime prior to and during the war. This strategy was later used in Ukraine during the annexation of Crimea and aggression in the eastern region. In the Georgian cyber-attack, website defacements included moving slideshows of images and slogans declaring the Georgian government and its officials were fascists. For example, the website of President Mikheil Saakashvili was defaced with a slideshow of the President and images of Adolf Hitler in mid-July 2008, see Figure 2.[67] A technical analysis of the graphic art used in the website defacement revealed that it had been created on 10 March 2006, when Russian-Georgian relations were strained. The U.S. Cyber Consequences Unit explains that “The graphic art was not deployed anywhere, however, but was

Figure 2

simply stored until it was used in the cyber campaign of August 2008."[68] The storage of the graphic art used in the website defacement as well as the extensive cyber reconnaissance efforts preceding the kinetic invasion of Georgia, suggests that the cyber element of the campaign had been planned well in advance.

Consistent with advanced planning, Russian media control mechanisms were in place for the conflict with Georgia. Much like during the Second Chechen War, media was strictly controlled. Deputy chief of the Russian Armed Forces General Staff, General Anatoliy Nogovitsyn commented on the situation, "Russian journalists stood united with the Russian army as never before, displaying heroism in covering the events in South Ossetia…finding the words and evidence to rebut torrents of lies and rejection, and helped the West to view our operations with understanding."[69]

However, "when the Russians invaded Georgia, a large portion of their military operations focused, not on securing the area inhabited by ethnic Russians, but on the Georgian ports and facilities for handling oil and gas. Unstable ground conditions, augmented by cyber-attacks, soon made all of the Georgian pipelines seem unreliable."[70] The value of Georgian oil transport networks was also affected by the disruption of the Turkish section of the Baku-Tbilisi-Ceyhan pipeline. While local militants claimed responsibility for the attack near Refahiye, reports surfaced that the disruption was actually a cyber-attack that exploited the lack of internal network monitoring of the pipeline's SCADA system. According to intelligence officials, hackers were able to exploit vulnerabilities in the pipeline's camera communication software in order to gain entry to the internal network. Having penetrated the network, the hackers were then able to disable the system "used to send alerts about malfunctions and leaks to the control room."[71] Many reported hearing an explosion at the time of the pipeline disruption, although no explosives were found.

Investigators believe the explosion was the result of the over-pressurization of crude oil. The failure of the back-up satellite signal alert system indicates that "the attackers used sophisticated jamming equipment" as well.[72] According to news reports:

> Although as many as 60 hours of surveillance video were erased by the hackers, a single infrared camera not connected to the same network captured images of two men with laptop computers walking near the pipeline days before the explosion, according to one of the people, who has reviewed the video. The men wore black military-style uniforms without insignias, similar to the garb worn by Special Forces troops.[73]

To further substantiate the cyber-attack theory, "investigators compared the time-stamp on the infrared image of the two people with laptops to data logs that showed the computer system had been probed by an outsider. It was an exact match."[74] The disruption of the Baku-Tbilisi-Ceyhan pipeline combined with the conflict in Georgia resulted in BP Azerbaijan's decision "to shift its oil transport to the Russian Baku-Novorossiysk pipeline, even though the costs were double those of the Georgian pipelines…The longer-term effect of these disruptions has been to cause oil producers to look for alternative routes."[75] The alternative routes more often than not, are Russian.

The 2008 Russian-Georgian War exemplified the use of information operations and cyber tools as force multipliers during a kinetic invasion. The information campaign against Ukraine is explored in the next section.

7. Russian Information Operations and Ukraine

The absence of military confrontation during the annexation of Crimea illustrates the value of influence operations to Russian military strategy. In April 2015, a Russian Defense Ministry source revealed that the government had created a special unit of the Information Operations Forces to be deployed in Crimea.[76] The unit was created in spring 2014 to be fully deployed by autumn 2015 with mission objectives including the "disruption of potential enemy's information

networks operation with the aim of incapacitating its troop command and control system [and] ensuring cybersecurity of the own information networks."[77] Prior to this announcement, NATO StratCom COE commented, "During the crisis in Ukraine, we have witnessed the application of a new type of warfare where dominance in the information field and hybrid, asymmetric warfare are the key elements."[78] The application of these elements contributed to the success of Russian operations "without open military conflict and deployment of large amounts of military power to the conflict area."[79] Cyber operations are a cornerstone of the Russian strategy in Ukraine. Like the information campaigns against Estonia and Georgia, the campaign against Ukraine uses cyber tools to spread disinformation and propaganda meant to destabilize the Ukrainian government and launch cyber-attacks against government websites, financial institutions, news agencies and other critical information nodes.

The Russian information campaign against Ukraine used state-supported narratives, reminiscent of those deployed in Estonia and Georgia, to criminalize and label local governments as fascist. "Control of narratives is seen as a more powerful tool than setting the media agenda, because recipients of the information reject those stories that contradict their "base narrative" or "strategic narrative". Narrative control means control over the process of interpreting information."[80] The pursuit of narrative control is not unique to Russian strategy. Lasting effects of the competition for narrative control is evidenced in the disputed memories of various conflicts around the world. One can achieve narrative control through the use of thematic communication frames. The thematic communication frames are used as part of social conditioning to train individuals to associate certain feelings or opinions with particular objects or subjects in a specified context. NATO StratCOM COE recorded Russian use of the following thematic narratives during the crisis in Ukraine:

- Socio-economic problems, dependency on Russia and the inability of the Ukrainian state to provide for its citizens/inhabitants;
- Radicalization of the opposition by positioning it either as a producer of opinions which may cause fear and panic within the community or as a laughing stock;
- Lack of social order and security used as a reason to justify Berkut's actions or the formation of the pro-Russian self-defense groups in East Ukraine;
- Euromaidan is a US/EU satellite and its supporters are traitors;
- The West is "evil" as it doesn't want to/can't save Ukraine from economic problems, is influencing the Ukrainian authorities in order to execute some conspiracy, inspires violence (like it does elsewhere in the world), is preparing extremists to cause public disorder in Ukraine (in particular, Lithuania and Poland are accused), promotes moral decadence;
- Russia is familiar to Ukraine but Western democracies are strangers;
- The common history of Russia and Ukraine, the Orthodox religion as a uniting element.[81]

These thematic communication frames were widely disseminated with the help of cyber tools and the Internet. The campaign simultaneously increased activity amongst pro-Russian and pro-Ukrainian hacking groups. For example leading hacker Yevhen Dokukin of the pro-Ukrainian group, the Ukrainian Cyber Troops, explained that the group used distributed denial of service attacks to render the Russian separatist proxies' websites inaccessible.[82] Groups such as the pro-Russian Cyber Berkut, masquerading as a pro-Ukrainian group claimed responsibility for the cyber attempts to disrupt parliamentary elections in Ukraine in 2014 as well as gaining access to confidential documents and correspondences of foreign governments.[83] The behavior of these groups and their role in the conflict deserve more attention.

Moscow's information operations in Ukraine used the Internet and various social media platforms to spread deliberately falsified information regarding the crisis in support of state-sponsored narratives. The use of disinformation and deception as a delaying tactic is a common element of the Russian influence campaigns. However, the value of disinformation erodes with time as others can disprove the falsified information. For example, the website www.stopfake.org is dedicated entirely to revealing the falsified information about the events in Ukraine.

An example of disinformation used as a delaying tactic pertains to the coverage of the Malaysia Airlines flight MH17 tragedy. The aircraft was shot down over the Russian separatist proxies' controlled Donetsk region. Russian news outlets published dozens of falsified variations of the story within 24 hours of the crash stating the Ukrainian government was responsible for the attack. With time, the value of the falsified accounts began to erode. However, disproving the falsified information required reallocating assets in a time of crisis to fact-check and publish correct reports.

Another example of deliberately falsified accounts is the Russian social media VKontakte's post by somebody pretending to be "Dr. Rozovkiy from Odessa". In the post, the "doctor" claimed that "pro-Ukrainian extremists" prevented him from helping victims of the trade union building fire in Odessa. He concluded his post by saying "In my city, such things did not happen even during the worst times of Nazi occupation. I wonder why the world is silent."[84] The post was translated into English, German, and Bulgarian and was shared more than 5,000 times in the first day. However, Radio Free Europe/Radio Liberty revealed that "Dr. Rozovkiy's profile picture is a photo of a North Caucasus dentist used in the advertising brochure of the *Ust Dzhegmiska Dental Clinic*."[85] The VKontakte post was removed shortly after the discovery. This is one example of numerous pro-Russian falsified posts across social media platforms. Like the overall Russian information operations strategy, Dr. Rozovkiy's post included references to fascism.

Furthermore, the visual material accompanying falsified posts reinforces the goals of the information campaign. Russian state television was an essential part of Russian information operations in Ukraine. Although, television is not within the scope of this paper, the online dissemination of Russian state television broadcasts deserves attention. It is important to note that the "Russian state TV's coverage of the conflict in Ukraine does not simply contain one-sided and

often misleading propaganda. It also appears to employ techniques of psychological conditioning designed to excite extreme emotions of aggression and hatred in the viewer."[86] The graphic imagery and accompanying music compounds the effects of the disinformation. For example, images from other conflict zones such as Syria and Chechnya have been passed off as happening in eastern Ukraine. These falsified images and films are broadcast on TV, as well as on social media platforms and online thereby expanding their reach and amplifying their effect. Psychological conditioning was also reinforced with DDoS attacks, website defacements, and pro-Russian trolling

7.1 Pro-Russian Trolling

Many people monitoring the discussions surrounding the Ukraine conflict in public online platforms are suspicious of the abundant pro-Russian trolling. "An internet troll is a person who foments discord online by starting arguments or upsetting people, by posting inflammatory, extraneous, or off-topic messages in an online community with the deliberate intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion."[87] Trolls typically maintain multiple fake or anonymous profiles. Some trolls work on behalf of organizations or groups that have developed a standard operating procedure. For example, "*Guardian* moderators, who deal with 40,000 comments a day, believe there is an orchestrated pro-Kremlin campaign."[88] Trolling and its value to Russian information campaigns is under-researched.

Radio Free Europe/ Radio Liberty (RFE/RL) reported that "there are thousands of fake accounts on Twitter, Facebook, LiveJournal, and VKontakte, all increasingly focused on the war in Ukraine."[89] Much of the activity has been linked to the Internet Research Center, one of Russia's

leading “troll factories.” Individuals work there in 12-hour shifts for salaries exceeding 40,000 rubles ($700) a month. RFE/RL recently interviewed professional Russian troll, Marat Burkhard. Burkhard explains that troll factories operate on production quotas, workers are required to post 135 comments no less than 200 characters a piece per 12-hour shift. When asked to describe a typical assignment, Burkhard provides the following post topic: “NATO troops are embedded with Ukrainian armed forces.”[90] He then would include the following keywords in each post related to the aforementioned topic: “Ukraine news, Russia and Ukraine, Ukraine policy, Ukraine, NATO, PMC (private military company).”[91] His task is to post inflammatory comments in a set number of forums. Various departments in the troll factory are responsible for initial posts, at which point workers in other departments can comment back. With each additional comment, keywords are included to turn up in search results along with references and links to other inflammatory posts. Trolls may work together or through multiple fake profiles to overwhelm other forum users. Here is an excerpt from a sample post Burkhard provided:

> The Kyiv junta regularly sics its media on Russia, and they lie shamelessly and recklessly. They argue Russian armed forces are fighting on the territory of Ukraine, but they refuse to provide any proof (because there isn't any). But when it comes to the matter of Ukrainian armed forces, the American puppets entrenched in Kyiv say there's no evidence that foreign mercenaries and Western intelligence agents are joining their ranks -- they lie and don't even blush![92]

The inflammatory intent of the message is clear. The value of trolling to disinformation campaigns is under-researched. However, the abundance of such comments can make others lose interest in participating in online forums. For example, *The Guardian* actively removes posts believed to be the work of trolls from the comment section of its articles and yet readers have written to the editors stating “In the past weeks [I] have become incredibly frustrated and disillusioned by your inability to effectively police the waves of Nashibot trolls who've been relentlessly posting pro-Putin propaganda in the comments on Ukraine v Russia coverage.”[93] While the role of Internet

trolling in the Russian information campaign against Ukraine is unclear, its overwhelming presence on public platforms suggests the malicious activity will be a component of conflicts Russia has a stake in, in the future.

7.2 Russian Special Operations Forces

Russian Special Operations Forces (SPETSNAZ) played a significant role in the information campaign against Ukraine. Their performance and equipment drastically improved from campaigns in Chechnya and Georgia. NATO StratCom COE's analysis of the SPETSNAZ performance in Ukraine, stated: "In Crimea, they conducted subversive actions in a silent and speedy manner, supporting the propaganda-driven partition of the community and the disruption of central government in a well-coordinated manner."[94] The presence of Russian troops and SPETSNAZ put immense psychological pressure on Ukrainian soldiers. As armed forces in unmarked Russian-issued green uniforms descended on Crimea, they took control of key government buildings and military bases and restricted the flow of information to the Ukrainian forces, government, and public. In Crimea, Ukrainian television and radio networks such as Black Sea TV were swiftly taken down and replaced with Russian channels while their online components were cyber-attacked. Russian military exercises near the Ukrainian border exerted further psychological pressure on the Ukrainian forces.

The armed men in unmarked uniforms came to be known as "little green men" or "polite people." With violence mounting and the number of victims growing in the eastern part of Ukraine, the "polite people" maintained a nonviolent appearance. News outlets around the world carried stories of the mysterious armed men taking control of strategic government and military installations in Crimea. The "polite people" simultaneously were the center of a strategically

coordinated social media campaign. Photographs of the armed men in Crimea posing with women and children, young girls and pets were trending on various social media platforms and garnering attention from international press. Keywords were used for easy online searching. The hashtags #politepeople, #Вежливыелюди and other spelling and capitalization variations in Russian and English were used. On social networking platforms a hash or pound sign (#) precedes a word or phrase to mark it as a keyword. Hashtags are easily searched and can provide valuable insight for analysts. For example, the use of hashtags was critical to Moldova's Twitter Revolution in 2009 and the Arab Spring.

The full effects of the "polite people" social media campaign are unclear. However, the online campaign supporting their presence in Crimea publicly integrated SPETSNAZ into the Russian information campaign. NATO StratCom COE explains that Russian information operations in Crimea "would not have been as successful and have brought such quick results without the well prepared Russian Special Operations Forces (so-called "polite men") on the ground who acted in accordance with the strategy to minimize bloodshed and apply strategic communication intent."[95]

8. Lessons from the Ukraine case

The Russian annexation of Crimea hints at a "new form of warfare where hybrid, asymmetric warfare, combining an intensive information campaign, cyber warfare and the use of highly trained Special Operation Forces, play a key role."[96] Russia exercised traditional information operations techniques of active measures and reflexive control to further achieve objectives in Ukraine. The union of these traditional methods with cyber tools and the Internet

along with the support of the SPETSNAZ contributed to the swift consolidation of power in Crimea.

The importance of information operations was solidified during the 18 March 2014 Kremlin meeting for the "official incorporation" of Crimea into the Russian Federation. The attendees included selected members of both houses of parliament, members of the Security Council and two leaders of Russian information operations theory and geopolitics, Igor Panarin and Aleksandr Dugin. The same day Panarin posted the following questionable information to his students in an online discussion group via VKontakte:

> **1.** It should be especially strongly emphasized that, in comparison to August 2008, Russia took many precautions in Crimea to prevent the planned violent scenario from being implemented.
> **2.** Russia has found a recipe to counteract the color revolutions which take the form of political coups.
> **3.** The world has been offered an alternative path of development, which is based on spiritual and ethical values.
> **4.** The Spirit of Valor has become crystallized: it has been possible to direct the accumulated impulse of Berkut's valor into the right channel.
> **5.** Russia's comprehensive actions on all fields of the counteraction of information (diplomatic, financial and economic, military, etc.) have been conducted in close coordination with and directed personally by Vladimir Putin.[97]

Panarin's post emphasizes the success of Russia's reformed information operations strategy. It is important to note that the Russian information campaign owes part of its success to the audience. Runet, or the Russian segment of the Internet "is a self-contained linguistic and cultural environment with well-developed and highly popular search engines, Web portals, social network sites, and free e-mail services. These sites and services are modeled on services available in the United States and the English-speaking world but are completely separate, independent, and only available in Russian."[98] Runet provided a way for the Kremlin to widely disseminate state-sponsored media directly to the Russian-speaking diaspora.

The importance of Russia's Compatriots Abroad policy should be evaluated. Passportization, the Russian practice of issuing Russian passports to individuals in other countries such as citizens of South Ossetia and Abkhazia in Georgia, was part of the takeover of Crimea. Moscow reserves the right to protect all Russian citizens; individuals who possess Russian passports. The Compatriots Abroad policy should be particularly concerning for countries neighboring Russia. The Kremlin's strategy for annexing Crimea would be best replicated in Russia's near abroad in countries that consume Russian-language media with large populations of Russian Compatriots Abroad.

The annexation of Crimea was made possible by Russia's influence operations in Ukraine. The dismal failure of Russian information operations during the First Chechen War prompted a series of reforms. The cyber-attack on Estonia, the war with Georgia, and the annexation of Crimea illustrate the growing role of the Internet and cyber tools in Russian information campaigns. After securing government, military and communication centers, cyber tools were used to promote support for the Russian campaign. It is likely that the success of the hybrid warfare techniques used in Ukraine will be used in future conflicts. Understanding the anatomy of Russian information operations is essential for crafting effective counter measures including cyber defense infrastructure and cybersecurity policy.

Endnotes

[1] Clausewitz, Carl von. *On War*, ed. and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976, 89.
[2] Winkler, Jonathan. "Information Warfare in World War I." *The Journal of Military History*, 73(3), 845.
[3] Thomas, "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?", 1.
[4] NATO Strategic Communications Center of Excellence (NATO StratCom COE), *Analysis of Russia's Information Campaign against Ukraine*. (2015), 32.
[5] Joint Chiefs of Staff. *Publication 3-13: Information Operations*. (2012), iii. Retrieved from: http://www.dtic.mil/doctrine/news_pubs/jp3_13.pdf

[6] Mann, Col Edward. "Desert Storm: The First Information War?." *Airpower Journal*. (1994).
[7] Issler, Gordon Major USAF. "Space war meets info war: The integration of space and information operations." Air Command and Staff College. 2000, 4.
[8] Thomas, Timothy. "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?" *Russian Military Reform 1992-2002*. (Frank Cass Publishers, 2003), 1.
[9] Ibid. 1.
[10] Darczewska, Jolanta. *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study*. (Warsaw: Centre for Eastern Studies, 2014), 9.
[11] Ibid. 12.
[12] Ibid.
[13] Panarin, Igor. *Vtoraya mirovaya informatsionaya voina – voina protiv Rossiya*. (Information World War II – War Against Russia) 2012.
[14] NATO StratCom COE, *Analysis of Russia's Information Campaign against Ukraine*, 46.
[15] Ibid. 45.
[16] Ibid. 41.
[17] Ibid.
[18] Dugin, Aleksandr. *Chetvertaya politicheskaya teoria*. (Fourth Political Theory). 2009.
[19] Thomas, Timothy. *Russia's Reflexive Control Theory and the Military*. (Journal of Slavic and Military Studies, 2004), 6.
[20] Blank, Stephen and Richard Weitz. *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*. (Pennsylvania: U.S. Army War College, 2010), 288.
[21] Ibid.
[22] United States Computer Emergency Readiness Team [USCERT]. *Security Tip ST04-015*. 2013.
[23] Ibid.
[24] Documents such as the Doctrine of Information Security of the Russian Federation (*Voyennaya Doktrina Rossiiskoy Federassi. Utverzhdena Ukazom Prezidenta RF ot 21 aprelya 2000 g. No. 706,* retrieved from: http://www.serf.gov.ru/Documents/Decree/2000706-1.html)
[25] Thomas, "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?," 5.
[26] Ibid.
[27]Denning, Dorothy. E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." Networks and Netwars: The Future of Terror, Crime, and Militancy (2001), 239.
[28]Ibid.
[29] Ibid.
[30] Ibid. 245.
[31] Thomas, "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?," 6.
[32] Ibid., 8
[33] Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol, California: O'Reilly Media, Inc. 2010, 162.
[34] *Voyennaya Doktrina Rossiiskoy Federassi. Utverzhdena Ukazom Prezidenta RF ot 21 aprelya 2000 g. No. 706,* retrieved from: http://www.serf.gov.ru/Documents/Decree/2000706-1.html
[35] Ibid., 222
[36] Thomas, "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?," 3.
[37] Russell, Allison Lawlor. *Cyber Blockades*. Georgetown: Georgetown University Press. 2014, 69.
[38] Heickero, Roland. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.* Stockholm: Swedish Defense Research Agency, Division of Defense Analysis, 2010, 39.
[39] Blank, Stephen. "Web War I: Is Europe's First Information War a New Kind of War?" Comparative Strategy (2008), 227.
[40] Lesk, Michael. "The New Front Line: Estonia under Cyberassault." Digital Protection (2007), 76.
[41] Blank, "Web War I: Is Europe's First Information War a New Kind of War?," 230.
[42]Ibid. 230.
[43] Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." Conference Proceedings of ECIW (2008), 124.
[44] Ibid. 125.
[45] Ibid. 123.
[46] Carr, *Inside Cyber Warfare*, 119.
[47] Ibid.
[48] Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, 38.

[49] Blank, Stephen. "Web War I: Is Europe's First Information War a New Kind of War?," 228.
[50] Ibid. 230.
[51] Ibid. 229.
[52] Ibid. 228.
[53] Ibid.
[54] Ibid.
[55] Ibid.
[56] Ibid., 232
[57] Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, 44.
[58] U.S. Cyber Consequences Unit. Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008. 2009, 3.
[59] Ibid.
[60] Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, 45.
[61] U.S. Cyber Consequences Unit. Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008, 13.
[62] Carr, Jeffrey. *Inside Cyber Warfare*, 109.
[63] Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, 46.
[64] U.S. Cyber Consequences Unit. Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008, 6.
[65] Ibid.
[66] Ibid., 5
[67] Georgian Ministry of Foreign Affairs. "Russian Cyberwar on Georgia." Russian Invasion of Georgia. 2008, 4.
[68]U.S. Cyber Consequences Unit. Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008, 5.
[69]Thomas, Timothy. "Russian Information Warfare Theory: The Consequences of August 2008." In The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald, edited by Stephen J. Blank and Richard Weitz, 265-299. Carlisle: Strategic Studies Institute, 2010, 238.
[70] U.S. Cyber Consequences Unit. Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008, 7.
[71] Robertson, Jordan and Michael Riley. "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar." Bloomberg Business, December 10, 2014. Accessed January 23, 2015. http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwarRobertson
[72] Ibid.
[73] Ibid.
[74] Ibid.
[75] U.S. Cyber Consequences Unit. Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008, 8.
[76] [93]Nevar, Vitaly. "Crimea to get separate unit of Information Operations Forces this autumn – source." *TASS Russian News Agency*, 2015. Accessed April 20, 2015. http://tass.ru/en/russia/790138
[77] Ibid.
[78] NATO StratCom COE, Analysis of Russia's Information Campaign against Ukraine, 32.
[79] Ibid.
[80] Ibid. 46.
[81] Ibid. 25-26.
[82] Shevchenko, Vitaly. "Ukraine conflict: Hackers take sides in virtual war." *BBC News*, 20 December 2014. Accessed 9 February, 2015. http://www.bbc.com/news/world-europe-30453069
[83] Ibid.
[84] NATO StratCom COE, Analysis of Russia's Information Campaign against Ukraine, 28.
[85] Ibid.
[86] Ennis, Stephen. "How Russian TV uses psychology over Ukraine." *British Broadcasting Company*, February 4, 2015. Accessed February 9, 2015. http://www.bbc.co.uk/monitoring/how-russian-tv-uses-psychology-over-ukraine
[87] NATO StratCom COE, Analysis of Russia's Information Campaign against Ukraine, 27.
[88] Elliott, Chris. "Ukraine Comment is free." *The Guardian*, May 4, 2014. Accessed February 9, 2015. http://www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online

[89] Volcheck, Dmitry and Daisy Sindelar. "One Professional Russian Troll Tells All." Radio Free Europe/Radio Liberty, 2015. Accessed March 26, 2015. http://www.rferl.org/content/how-to-guide-russian-trolling-trolls/26919999.html
[90] Volchek and Sindelar, "One Professional Russian Troll Tells All."
[91] Ibid.
[92] Ibid.
[93] Elliott, "Ukraine Comment is free"
[94] NATO StratCom COE, Analysis of Russia's Information Campaign against Ukraine, 35.
[95] Ibid. 33.
[96] Ibid. 4.
[97] Darczewska, Jolanta, "The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study," 23-24.
[98] Deibert, R. and Rohozinski, R. "Control and Subversion in Russian Cyberspace." In Access Controlled: The shaping of power, rights, and rule in cyberspace, edited by John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, 15-34. Cambridge: MIT Press, 2010, 19.

Bibliography

Applegate, Scott. "Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare." Security & Privacy. (2011): 16-22

Blank, Stephen. "Web War I: Is Europe's First Information War a New Kind of War?" Comparative Strategy (2008): 227-247.

Carr, Jeffrey. Inside Cyber Warfare. Sebastopol, California: O'Reilly Media, Inc. 2010.

Clausewitz, Carl von. *On War*, ed. and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Darczewska, Jolanta. "The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study." Warsaw: Centre for Eastern Studies, 2014.

Deibert, R. and Rohozinski, R. "Control and Subversion in Russian Cyberspace." In Access Controlled: The shaping of power, rights, and rule in cyberspace, edited by John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, 15-34. Cambridge: MIT Press, 2010.

Denning, Dorothy. E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." Networks and Netwars: The Future of Terror, Crime, and Militancy (2001): 239-288.

Dugin, Aleksandr. *Chetvertaya politicheskaya teoria*. (Fourth Political Theory). 2009.

Elliott, Chris. "Ukraine Comment is free." The Guardian, May 4, 2014. Accessed February 9, 2015. http://www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online

Ennis, Stephen. "How Russian TV uses psychology over Ukraine." British Broadcasting Company, February 4, 2015. Accessed February 9, 2015. http://www.bbc.co.uk/monitoring/how-russian-tv-uses-psychology-over-ukraine

Georgian Ministry of Foreign Affairs. "Russian Cyberwar on Georgia." Russian Invasion of Georgia. 2008.

Heickero, Roland. Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. Stockholm: Swedish Defense Research Agency, Division of Defense Analysis, 2010.

Issler, Gordon Major USAF. "Space war meets info war: The integration of space and information operations." Air Command and Staff College. 2000.

Joint Chiefs of Staff. Publication 3-13: Information Operations, 2012. Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

Joubert, Vincent. "Five years after Estonia's cyber-attacks: lessons learned for NATO?" NATO, 2012.

Lesk, Michael. "The New Front Line: Estonia under Cyberassault." Digital Protection (2007): 76-79.

Mann, Col Edward. Desert Storm: The First Information War? Airpower Journal, 1994.

NATO StratCom COE. Analysis of Russia's Information Campaign against Ukraine. NATO, 2015. Accessed February 16, 2015. http://www.stratcomcoe.org/~/media/SCCE/NATO_PETIJUMS_PUBLISKS_29_10.ashx

Nevar, Vitaly. "Crimea to get separate unit of Information Operations Forces this autumn – source." TASS Russian News Agency, 2015. Accessed April 20, 2015. http://tass.ru/en/russia/790138

Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." Conference Proceedings of ECIW (2008): 119-131

Panarin, Igor. *Vtoraya mirovaya informatsionaya voina – voina protiv Rossiya*. (Information World War II – War against Russia) 2012.

Robertson, Jordan and Michael Riley. "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar." Bloomberg Business, December 10, 2014. Accessed January 23, 2015. http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

Russell, Allison Lawlor. *Cyber Blockades*. Georgetown: Georgetown University Press. 2014.

Shevchenko, Vitaly. "Ukraine conflict: Hackers take sides in virtual war." *BBC News*, 20 December 2014. Accessed 9 February, 2015. http://www.bbc.com/news/world-europe-30453069

Thomas, Timothy. "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?" Russian Military Reform 1992-2002 (2003): 209-233.

Thomas, Timothy. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Military Studies* (2004): 237-256.

Thomas, Timothy. "Russian Information Warfare Theory: The Consequences of August 2008." In The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald, edited by Stephen J. Blank and Richard Weitz, 265-299. Carlisle: Strategic Studies Institute, 2010.

Tikk, Eneken et al. Cyber Attacks Against Georgia: Legal Lessons Identified. NATO: Cooperative Cyber Defense Center of Excellence, 2008.

U.S. Cyber Consequences Unit. Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008. 2009.

United States Computer Emergency Readiness Team. “Security Tip (ST04-015): Understanding Denial-of-Service Attacks.” United States Computer Emergency Readiness Team, 2013. Accessed April 15, 2014. http://www.uscert.gov/ncas/tips/ST04-015

Voyennaya Doktrina Rossiiskoy Federassi. Utverzhdena Ukazom Prezidenta RF ot 21 aprelya 2000 g. No. 706, retrieved from: http://www.serf.gov.ru/Documents/Decree/2000706-1.html

Volcheck, Dmitry and Daisy Sindelar. “One Professional Russian Troll Tells All.” Radio Free Europe/Radio Liberty, 2015. Accessed March 26, 2015. http://www.rferl.org/content/how-to-guide-russian-trolling-trolls/26919999.html

Winkler, Jonathan. “Information Warfare in World War I.” The Journal of Military History, 73(3), 845.