Fear, Honor, Interest: An Analysis of Russia's Operations in the Near Abroad (2007-2014)

A Monograph

By

MAJ Antonius J.C. Selhorst
Royal Netherlands Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

AY 2015-001

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
05-21-2015	Monograph	JUN 2014 – MARCH 2015

4. TITLE AND SUBTITLE
Fear, Honor, Interest: An Analysis of Russia's Operations in the Near Abroad (2007-2014)

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major Antonius JC Selhorst
Royal Netherlands Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies 250 Gibbon Ave Ft. Leavenworth, KS 66027

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Command and General Staff College
250 Gibbons
Ft. Leavenworth, KS 66027

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In recent years, Russia has conducted several operations in former Soviet states, attempting to halt NATO expansion and protecting ethnic Russian minorities in those states. Western analyses have focused either on traditional military means in these operations or on novelties in the cyber domain, but rarely have they used these approaches with others. They focused especially on what lessons Russia learned from them to reform their armed services. This is a very narrow analysis, based on Western assumptions on the Russian way of war. Instead, Russia has created a new operational concept, which it refers to as "the fifth period of operational art," especially designed for its near-abroad policy. This new operational concept uses traditional domains with military means, non-traditional domains such as the human, information, and cyber domain, and non-military means such as (cyber) proxy forces linked to the social conditions of Russians living as minorities outside Russia. This monograph reviews the changes, their background, and practical application, together with their links to the social conditions of ethnic Russian minorities in former Soviet states. First, it describes the history of the collapse of the Soviet Union, the fate of the 25 million displaced ethnic Russians, their marginalization, regional tensions, and the strategy that Russia has developed to protect these ethnic Russians and its interests in the near abroad. Next, this monograph reviews the theory on the fifth period of operational art and creates an operational framework based on the theory and case studies of the 2007 Estonia crisis, 2008 Georgia war, and 2014 Ukraine conflict. Finally, it reveals how this framework uses non-military means linked to social conditions.

15. SUBJECT TERMS
Russia, Operational Art, Human Domain, Cyber Domain, Reflexive Control, Information Warfare, Social Sciences, Moldova, Estonia, Georgia, Ukraine, Nashi, Whole of Society

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Maj Antonius JC Selhorst
(U)	(U)	(U)	(U)	66	**19b. PHONE NUMBER** *(include area code)*

Monograph Approval Page

Name of Candidate: Major Antonius J.C. Selhorst

Monograph Title: Fear, Honor, Interest: An Analysis of Russia's Operations in the Near Abroad (2007-2014)

Approved by:

_____, Monograph Director
Christopher Marsh, PhD

_____, Seminar Leader
James W. MacGregor, COL

_____, Director, School of Advanced Military Studies
Henry A. Arnold III, COL

Accepted this 21st day of May 2015 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, PhD

The opinions and conclusions expressed herein are those of the student author, and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

Abstract

Fear, Honor, Interest: An Analysis of Russia's Operations in the Near Abroad (2007-2014), by Major Antonius J.C. Selhorst, Royal Netherlands Army, 66 pages.

In recent years, Russia has conducted several operations in former Soviet states, attempting to halt NATO expansion and protecting ethnic Russian minorities in those states. Western analyses have focused either on traditional military means in these operations or on novelties in the cyber domain, but rarely have they used these approaches with others. They focused especially on what lessons Russia learned from them to reform their armed services. This is a very narrow analysis, based on Western assumptions on the Russian way of war. Instead, Russia has created a new operational concept, which it refers to as "the fifth period of operational art," especially designed for its near-abroad policy. This new operational concept uses traditional domains with military means, non-traditional domains such as the human, information, and cyber domain, and non-military means such as (cyber) proxy forces linked to the social conditions of Russians living as minorities outside Russia. This monograph reviews the changes, their background, and practical application, together with their links to the social conditions of ethnic Russian minorities in former Soviet states. First, it describes the history of the collapse of the Soviet Union, the fate of the 25 million displaced ethnic Russians, their marginalization, regional tensions, and the strategy that Russia has developed to protect these ethnic Russians and its interests in the near abroad. Next, this monograph reviews the theory on the fifth period of operational art and creates an operational framework based on the theory and case studies of the 2007 Estonia crisis, 2008 Georgia war, and 2014 Ukraine conflict. Finally, it reveals how this framework uses non-military means linked to social conditions.

Table Of Contents

Acronyms

CIS	Commonwealth of Independent States
EU	European Union
NATO	North Atlantic Treaty Organization
RFAF	Russian Federation Armed Forces
US	United States
USSR	Union of Soviet Socialist Republics

Figures

Tables

Introduction

> Currently we are in the fifth period in the development of operational art.
> —V.K. Kopytko, *Voyennaya Mysl [Military Thought]*

In recent years, Russia has conducted operations in former Soviet states to prevent the North Atlantic Treaty Organization (NATO) from expanding its sphere of influence into areas formerly part of the Union of Soviet Socialist Republics (USSR).[1] Western analyses of these conflicts have focused on the means Russia has deployed to achieve its goals in these conflicts: cyber forces in Estonia, conventional forces in Georgia, and special operations forces (SOF) in Ukraine. Western analysts especially studied the Russian Federation Armed Forces' (RFAF) lessons of their operations and the way they complemented their conventional military with SOF, airborne, and naval infantry as rapid reaction forces. These analysts also speculate about how Russia would use cyber in future conflicts.[2] These analyses are too narrow and based on Western assumptions on the Russian way of war, using military means within the traditional domains of air, sea, and land, expanded with the new cyber domain.

In contrast, the RFAF has changed its way of war into an operational concept built on the human concepts of fear, honor, and interest that include engagement in the human and cyber domains with non-military means to achieve Russian objectives, protecting Russian minorities abroad. The RFAF has focused on social conditions and complex environments and applied different approaches in order to assist in the development of situationally unique planning

---

[1] Foreign Broadcast Information Service Central Eurasia, "Military Doctrine of the Russian Federation 2010," accessed 10 July 2014, http://news.kremlin.ru/ref_notes/461.

[2] Ariel Cohen and Robert E. Hamilton, "The Russian Military and the Georgian War: Lessons and Implications" (Monograph, Strategic Studies Institute, U.S. Army, Carlisle, PA, 2011); Roland Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations* (Stockholm, Sweden: Swedish Defence Research Agency, 2010).

models.[3] These models apply military and non-military means such as SOF, proxy forces, civil media, and cyber capabilities to influence all actors, provoke reactions, disturb communication, and destabilize regions in order to achieve its objectives. To create the non-military means, Russia established civilian capabilities such as youth groups and state media, and mobilized Russian ethnic minorities abroad by appealing to feelings of marginalization (fear), a sense of self-worth and belonging (honor), and a perception that Mother Russia has more to offer than the native country (interest). These developments make the Russian operational concept a whole-of-society approach.

Changes to means and domains are not new for Russian operational concepts as they evolved since 1920 in five distinct periods, although the principles, foundations, and tenets of the overarching operational art largely remained the same.[4] In the first period, between 1920 and 1940, the operational concept encompassed front-scale and army-scale operations. The second period, which lasted until 1953, emphasized deep battle in combination with overwhelming firepower. Nuclear arms and missiles defined the third period, which ran from 1954 to 1985, while the fourth period, lasting until 2000, focused on the use of high-precision arms. Vasily Kopytko, professor at the Operational Art Department of the General Staff Academy, defined the last shift towards non-military means and non-traditional domains in the operational concept as the fifth period of Russian operational art.[5]

---

[3] Michael R. Gordon, "Russia Displays a New Military Prowess in Ukraine's East," *The New York Times*, 21 April 2014, accessed 2 July 2014, http://www.nytimes.com/2014/04/22/world/europe/new-prowess-for-russians.html?_r=0.

[4] Vasily K. Kopytko, "Evolution of Operational Art," *Voyennaya Mysl* 17, no 1 (2008): 202-214.

[5] A. V. Smolovyi, "Problemniye voprosy sovremennogo operativnogo iskusstva i puti ikh rescheniya," *Voyennaya Mysl* no. 12 (2012): 21-24; Valery Gerasimov, "The value of science in anticipation," *VPK news*, 27 February 2014, accessed 2 July 2014, http://www.vpk-news.ru/articles/14632.

The Russian shift in means and domains pose a challenge to the Western way of war. To understand contemporary RFAF operational approaches better, this monograph explores the use by Russia of non-military means based on social conditions, by asking: "How does the Russian Federation use non-military means linked to social conditions in its current operational art?" The relevance of this monograph is twofold. First, to help NATO to understand the new Russian operational concept so it can anticipate the possible and prepare for the probable. Second, NATO can benefit from this monograph to refine its approach towards the new Russian way of war. A first draft of the counter-unconventional warfare identifies some of the means the RFAF use, but fails to focus on the dependence between the non-military means and social conditions.[6]

Methodology

This monograph contains three sections on theory, practice, and analysis and creates a Russian operational framework. The first section explores the social and strategic context, as well as the theoretical background of Russian operational art, through a literature review. The social context describes the living conditions of ethnic Russians outside of Russia after the collapse of the USSR, which Russia uses as a pretext of its operations. The strategic context describes the conditions under which national strategy has evolved and what national objectives it pursues. The literature review of current and previous Soviet and Russian operational concepts, referred to as periods of operational art, describe lasting principles, foundations, and tenets used to construct a preliminary operational framework based on the assumption that already ingrained principles in an organization are hard to escape.[7]

---

[6] Department of the Army, *Counter-Unconventional Warfare* (Washington, DC: Department of the Army, 2014).

[7] Peter L. Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (New York: Doubleday, 1966).

The second section uses this preliminary operational framework to explore the use of non-military means linked to social conditions by Russia in previous conflicts. It contains case studies on the Estonia, Georgia, and Ukraine conflicts, and gives insight to complement the current Russian operational framework.[8] This section uses the 2007 Estonia crisis and 2008 Georgian conflict because Russia expert Stephen Blank claims that current Russian strategy and doctrine are the result of debates that took place in the 2003-2006 period. [9] This means that the RFAF refined its current operational concept with their results. Additionally, the Georgia case study is interesting as Russia created a Russian minority to protect in two breakaway regions, indicating that Russia also uses the new approach in areas without Russian minorities. An in-depth case study of the recent Ukraine conflict further refines the framework to see if events unfolded in a predictable way, and to explore how Russia used social conditions within this framework. This final case study on Ukraine is limited to the Crimea conflict, as there is not enough literature available to include the ongoing conflict in Eastern Ukraine.

The third section is a synthesis of the previous two sections and delivers a generic operational framework, with an emphasis on non-military means linked to social conditions. The concluding section answers the primary question, "How does the Russian Federation use non-military means linked to social conditions in its current operational concept?" and provides recommendations for further research.

---

[8] Stephen van Evera, *Guide to Methods for Students of Political Science* (Ithaca: Cornell University Press, 1997).

[9] Blank, Stephen J., "No Need to Threaten Us, We Are Frightened of Ourselves: Russia's Blueprint for a Police State, The New Security Strategy," in *The Russian Military Today and Tomorrow - Putin, Russian Navy, Ukraine, Gazprom, Rosneft, Lavrov, Deep Operations, Campaign Design, Russian-Chinese Security Relations, Mafia and Arms Dealers*, eds Stephen J. Blank and Richard Weitz (Carlisle PA: Strategic Studies Institute, U.S. Army, 2014), 305-1100, Kindle ed.

Figure 1. Countries and regions

Source: Courtesy of the University of Texas Libraries. The University of Texas at Austin, "European Union," University Of Texas Libraries, accessed 10 December 2014, http://www.lib.utexas.edu/maps/cia14/european_union_sm_2014.gif. Adapted by author to illustrate conflict zones in former Soviet space.

Definitions and Limitations

This monograph uses US Army and joint doctrine definitions and common civil or Russian military definitions for those terms not present in US doctrine. The most prominent definition of this monograph is that of the human domain as "the totality of the cognitive, information, social, cultural, and physical elements affecting and influencing human behavior."[10] In the human domain, a military uses social facts and conditions concerning history, culture, linguistics, sociology, communication, human geography, political science, public administration, and psychology to engage with actors on all levels.[11] An actor is an individual or group within a

[10] F. G. Hoffman and T. X. Hammes, *Joint Force 2020 and Human Dynamics: Time for a New Conceptual Framework?* (Washington, DC: Center for Strategic Research, National Defense University, 2013), 22.

[11] Hriar Cabayan et al., *Operational Relevance of Behavioral and Social Science to DoD Missions* (Washington, DC: NSI Team, 2013), 7.

society who acts to advance personal interests. They include individuals, states and governments, coalitions, terrorist networks, and criminal organizations.[12] Though the cyber domain is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers," this monograph explores *influence activities* in the cyber domain as part of the human domain.[13]

Many Russian strategic-level documents (unclassified) are public and available in English. Using RFAF sources is problematic as Russian sources are either scarce or classified and the group of Western experts on Russian operational art is small. This research therefore relies on published studies and articles from think tanks and universities, such as the Foreign Military Studies Office, Strategic Studies Institute, US Army School for Advanced Military Studies, US Army War College, National Defense University, and the Latvian Defense Academy. It uses news websites such as the British Broadcasting Corporation, *The Guardian*, *Nederlandse Omroep Stichting* [Netherlands Broadcasting Foundation], and regionally pecialized websites such as EastView Press to complement the studies and articles.

[12] Army Doctrine Reference Publication (ADRP) 5-0, *The Operations Process* (Washington, DC: Department of the Army, 2012), 2-7.

[13] Joint Publication (JP) 1.02, *Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense, 2013), 67.

Section 1

Background, Strategy, and Operational Art

> The strategic purpose of war is to attain a better condition of peace.
>
> —Carl Von Clausewitz, *On War*

Russian security strategy and operational concept did not evolve in a vacuum during the past decade, but are a reaction to events that unfolded after the collapse of the USSR. First, this evolution is a reaction of Russian leadership under President Vladimir Putin to counter the diminishing role of Russia in its traditional sphere of influence and the increasing role of the United States of America and NATO in that sphere. Second, this evolution is a reaction to the concerns of the Russian population and Russian Orthodox Church on the fate of 25 million ethnic Russians living outside Russia, their marginalization, and regional crises in the 1990s.[14] These crises provided Russia with lessons on how to use non-military means and social conditions for their operational concept, while at the same time the displaced Russians provided Russia's leadership with an excuse to re-establish its influence and a means to mobilize its society for conflict. The first subsection therefore describes the social context in which the operational concept has evolved.

Social Context

Unrest in the USSR started in mid-1989 with demonstrations and clashes between ethnic minorities, after which the first Soviet states became independent.[15] Discontent over living conditions under communist' rule, topped by an economic crisis that most blamed on Moscow,

---

[14] Nikolas K. Gvosdev and Christopher Marsh, *Russian Foreign Policy Interests, Vectors, and Sectors* (Thousand Oaks, CA: CQ Press, 2014), 164.

[15] Gvosdev and Marsh, 163; Robert Service, *A History of Modern Russia from Nicholas II to Vladimir Putin* (Cambridge, MA: Harvard University Press, 2005), 481.

and a desire for regaining independence finally led to the collapse of the USSR in December 1991.[16] The leaders of Belarus, Russia, and Ukraine initiated the Commonwealth of Independent States (CIS) as an overarching military and economic entity, meant to foster cooperation in the political, economic, and social spheres among its members. Given the formation of the CIS simultaneously with the collapse of the Soviet Union, the status of ethnic Russians outside Russia seemed secured.[17] This later proved to be naïve. All former Soviet states joined the CIS eventually except for the Baltic States. At the same time, some ethnic Russians outside of Russia began to raise the issue of redrawing Russia's borders to include them within a greater Russia. This almost immediately led to tensions, civil disturbance, and civil wars, most notably in Chechnya.[18]

The first civil war outside Russia started in 1991 when Moldova became independent from the USSR and sought reunification with Romania.[19] This was against the interest of Moscow because Moldova contained large Soviet-era military storages, while Moldova's third largest group of inhabitants were ethnic Russians.[20] A civil war started with the declaration of independence of Transnistria, a province of Moldova separated from the rest of the country by the Dniester River and inhabited largely by ethnic Russians.[21] These Russians did not want to adopt

---

[16] Gvosdev and Marsh, 163-164; Service, 468.

[17] Gvosdev and Marsh, 163-164.

[18] Ibid.; Moshe Gammer, *The Lone Wolf and the Bear: Three Centuries of Chechen Defiance of Russian Rule* (Pittsburg, PA: University of Pittsburg Press, 2006), 200-218.

[19] Nicole J. Jackson, *Russian Foreign Policy and the CIS: Theories, Debates, and Actions* (London, UK: Routledge, 2003), 89.

[20] Stephen Blank, "Russian Threats to Moldova and the Balkans," *Central Europe Digist* (9 May 2014): 10; Matthew Crandall, "Hierarchy in Moldova-Russia Relations: The Transnistrian Effect," *Studies of Transition States and Societies* 4, no. 1 (2014): 6.

[21] Organization for Security and Co-operation in Europe (OSCE), "Transdniestrian Conflict, Origins and Main Issues," *OSCE*. 10 June 1994, accessed 22 August 2014. http://www.osce.org/moldova/42308?download=true, 2.

the Romanian-Moldovan language as the Moldovan government wanted, but remained loyal to their Russian background.[22] They seized governmental, communications, economic, and security forces infrastructure in Transnistria as the Moldovan Army reacted in an attempt to stop the separatists.[23]

Russian media and diplomats targeted national and international perceptions that Moldova was the aggressor and was attempting to commit genocide against Russian minorities.[24] Russian leadership started building a coalition with the separatists, while the 14th Army, still present in Transnistria to guard the Soviet-era military equipment, started to arm the separatists. Cossack and Spetznaz units[25] from the USSR deployed rapidly to support the separatists and 14th Army.[26] At this point, the separatists had a force larger than the whole Moldovan Army inside the breakaway region and the occupation of Transnistria by the separatists was a *fait accompli*.[27] This provoked an attack by the Moldovan Army that the 14th Army repelled in a short war between 17 and 22 June 1992.[28] This display of Russian power forced Moldova into a peace settlement, the

---

[22] Matthew Crandall, "Hierarchy in Moldova-Russia Relations: the Transnistrian Effect," *Studies of Transition States and Societies* 4, no. 1 (2014): 4.

[23] Jackson, 82.

[24] Jackson, 97-98.

[25] Spetsnaz, or *voiska spetsial'nogo naznacheniya*, are "forces of special designation," often equated with US Special Forces. Specific units such as *Vympel* conduct unconventional warfare. Cossack units are comprised of volunteers of ethnic Cossacks, a people with a historical bond to Russia that seek the restoration of the Russian Empire.

[26] Jackson, 92-95.

[27] Mihai-Cristian Statie, "Transnistria: The 'Hot' Nature of a 'Frozen' Conflict" (Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2013), 10-34; Jackson, 102.

[28] Statie, 10-34; OSCE, 2.

latter agreeing to accept CIS peacekeeping forces.[29] Moldova would not be the only crisis, but gave Russia valuable lessons on how to use social conditions and paramilitary forces.

As in Moldova, most former Soviet states contain an ethnic Russian minority that either lived as a minority intermingled with natives or as a regional majority. The new governments pursued pro-Western policies to counter Russian influence, provide security against a Russian threat, and pursue economic prosperity for their nation.[30] Due to animosity caused by the previous Russian occupation, many states adopted legislation in their countries restricting the civil rights of ethnic Russians.[31] In many cases, the Russian language was no longer an official language and ethnic Russians had to learn the country's language in order to gain citizenship.[32] If they were unable to comply, they could not apply for better-paid jobs; many lost their jobs anyway because of ethnic discrimination.

These developments created a lower social class group, caused a feeling of marginalization and discrimination, and led ethnic Russians to cling to their Russian identity, language, culture, and religion. This helped their self-confidence and sense of self-worth, created involvement in social activity, developed community networks, and provided a forum to explore personal rights.[33] This new religious and cultural revival of Russia started in 1988, together with a new sense of the Great Russian Empire that defeated Nazi Germany.[34] The Russian Orthodox

---

[29] Information Handling Services (IHS) Jane's, *Jane's Sentinel Security Assessment - Russia And The CIS* (Englewood, CO: IHS Global Limited, 2014), 13; Statie, 10-34; Jackson, 96.

[30] Jackson, 82.

[31] Victor Shnirelman, "New Racism, Clash of Civilisations and Russia," in *Russian Nationalism and the National Reassertion of Russia*, ed. Marlene Laruelle (Abingdon, UK: Routledge, 2009), 136-166.

[32] Shnirelman, 136-166; Service, 482.

[33] Yael, Ohana, *Supporting Cultural Actors of Change in Belarus, Moldova and Ukraine: A Regional Review* (Washington, DC: The German Marshall Fund of the United States, 2008), 9.

[34] Service, 476-493.

Church started to support the ethnic Russians abroad and became a player in Russian politics as it created a picture of a pure Orthodox Russia that geographically extended well beyond Russia's current borders, often including Ukraine itself.[35] Within the Russian Orthodox Christian community, new forms of anti-Semitism, intolerance towards homosexuals, and xenophobia had matured and when combined with nationalism and marginalization, led to extremist fascist groups.[36] Some of these groups were a source for youth groups whose sole purpose was to protect the motherland, especially against NATO and former Nazi-collaborators, former Soviet states that supported Nazi Germany in World War II at the expense of Russia.[37]

On top of these developments came NATO's expansion to the east, gradually moving the Alliance to the Russian border in 2004 with the incorporation of the Baltic States. These developments, socially and politically, together with the lessons of the Moldova conflict, redefined Russia's strategic goals and ways to pursue them.

National Strategy and Military Doctrine

Beginning early 2000, Russia began to pursue a near-abroad policy establishing a sphere of influence in the former Soviet States, to protect Russian interests and ethnic Russian minorities abroad.[38] After the Baltic States joined NATO and the European Union (EU) in 2004, this near-abroad policy evolved into an approach to prevent any other former Soviet states from joining the

---

[35] Christopher Marsh, "Orthodox Spiritual Capital and Russian Reform," in *The Hidden Form of Capital*, eds.Peter Berger and Gordon Redding (London, UK: Anthem Press, 2010), 175; Christopher Marsh, "Eastern Orthodoxy and the Fusion of National and Spiritual Security," in *The Routledge Handbook of Religion and Security,* eds. Chris Seiple, Dennis R. Hoover and Pauletta Otis (Abingdon, UK: Routledge, 2013), 22-28.

[36] Marsh, "Eastern Orthodoxy," 22-28.

[37] Marlene Laruelle, "Negotiating History, Memory Wars in the Near Abroad and Pro–Kremlin Youth Movements," *Demokratizatsiya* [Democratization] 8, no. 4 (2000): 233-252.

[38] Gvosdev and Marsh, 157.

EU and/or NATO.[39] This approach defines current Russian strategy, which is a combination of national security strategy and military doctrine that define Russia's strategic ends, ways, and means. Maintaining the Russian sphere of influence in the near abroad is the Russian strategic end state that defines a set of comprised objectives.[40]

Russian security strategy and military doctrine radically transformed with Putin's rise to power. The 2000 *National Security Strategy* was a clear warning to NATO that Russia would not let NATO intervene in former Soviet states as it did in the Balkans, and suggesting Russia would use nuclear weapons as a defensive weapon again.[41] In 2003, Putin released a white paper, *The Priority Tasks of the Development of the Armed Forces of the Russian Federation,* and in 2009, the Russians updated their *National Security Strategy* policy. [42]

These policies led to a significant change in national military doctrine that reflected the security situation at that time and focused on internal conflicts.[43] Based on the 1991 Iraq Gulf War, Russian military thinkers argued that future war would be a non-contact war, one without engaging enemy forces in a traditional way.[44] Warfare would shift towards the use of precision guided ammunitions, standoff weapons, and information warfare, i.e. "actions and measures used both in preparations for and during war to achieve strategic supremacy over an enemy in the

---

[39] Marcel de Haas, "Russia's Military Doctrine Development (2000-2010)," in *Russian Military Politics and Russia's 2010 Defense Doctrine,* ed. Stephen J. Blank (Carlisle, PA: Strategic Studies Institute, U.S. Army, 2011), 10-15, 51.

[40] Joint Publication (JP) 5-0, *Joint Operation Planning* (Washington, DC: Department of Defense, 2014), III-21.

[41] Gvosdev and Marsh, 129-130.

[42] Military Doctrine of the Russian Federation; Ministry of Defense, *The Priority Tasks of the Development of the Armed Forces of the Russian Federation* (Moscow: The Defense Ministry of the Russian Federation, 2003), 59-61.

[43] De Haas, "Russia's Military Doctrine Development," 7

[44] Mattson and Eklund, 37.

information sphere by influencing its information and communication means, as well as state and military control systems and objects."[45] Next, experts saw the deployment of peacekeeping forces to Kosovo as a means to ensure Russia had a voice in the peace settlement.[46]

The white paper supported this change in military thinking and defined a new concept for Russian operational art based on the integration of strategic, operational, and tactical elements, whereby exploitation of strategic advantages come first, to be followed by deployment of troops to vital territory.[47] Highly mobile forces would cause operational effects. Vital to the new strategy was the swift destruction, disruption, or control of communications, economics, infrastructure, and political institutions to disrupt command and control of the enemy. Another target was the population, either to use as a proxy force or to isolate from their leaders, based on the Moldova experience. Key was deception related to policy, military action, and preparations. The white paper emphasized the use of proxy forces, cyber, and electronic warfare.[48]

The Russian security strategy of 2009 reflected this change. First, the strategy stated that Russia must ignore international laws and institutions, with military force again being valuable for settling conflicts.[49] Second, external threats to Russia mainly came from NATO, which used diplomatic, economic, and informational pressure together with subversive activities and interference in internal affairs to break up Russia and the CIS. The Russian Government, therefore, created an independent directorate, part of the Presidential Staff, to direct all

---

[45] Jacob W. Kipp, "Russian Military Doctrine: Past, Present, and Future," in *Russian Military Politics and Russia's 2010 Defense Doctrine*, ed. Stephen J. Blank (Carlisle, PA: Strategic Studies Institute, U.S. Army, 2011), 99; Thomas, 146.

[46] Kipp, "Russian Military Doctrine," 96.

[47] Mattson and Eklund, 40; De Haas, "Russia's Military Doctrine Development," 14.

[48] Mattson and Eklund, 40; Joint Publication (JP) 1.02, *Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense, 2013), 88.

[49] Stephen J. Blank, "No Need to Threaten Us," 470-685, Kindle ed.

information activity to shape Russia's favorable image and counter these threats.[50] Finally, the security strategy embraced a whole-of-society approach that resulted in the use of national and regional media by the military to conduct information warfare. To overcome departmentalism within the government and improve the quality of strategic planning, President Dmitry Medvedev enhanced the position of the Security Council.[51]

The 2003 white paper and the 2009 *National Security Strategy* formed the bases for the 2010 *National Military Doctrine.* The new doctrine described the necessity for Russia to send troops abroad to protect national interests or Russian citizens along the country's perimeter. The doctrine also described the use of non-military means such as information warfare.[52] Russia had to prepare for conflicts, to gain strategic initiative that would lead to victory, seeking superiority in the physical and information domains, building the ability to strike with precision, by neutralizing, not destroying the opposing forces, and then consolidating military gains with diplomatic and other political means. Information attack and defense would dominate and support the strategic initiative. Political success, even limited, would ensure continuity of the strategy.[53]

The message of the policy papers supported the near-abroad policy. Former Soviet states should choose Russia's side or remain neutral and NATO and the EU must accept Russia's position as a regional power.[54] Experts give comparable reasons for Russian policy statements and activity, linked to non-acceptance of the collapse of the USSR, with a ruling elite that uses power for their own gains. These experts argue that the real end state is restoration of the former

---

[50] Blank, "No Need to Threaten Us," 457-556, Kindle ed.

[51] Ibid., 685-1003, Kindle ed.

[52] De Haas, "Russia's Military Doctrine Development (2000-2010)," 44.

[53] Kipp, "Russian Military Doctrine: Past, Present, and Future," 105-111.

[54] Ibid, 105-111; Gvosdev and Marsh, 157.

USSR, including all Slavic countries.[55] Although this seems farfetched, the real ends of Russia's policy probably contain a mix of the near-abroad policy and expansion of territory, the latter in support of the former, to establish a strong CIS as replacement of the USSR.[56] The policy papers describe the ways and means to reach these end states that led Russia to redefine its operational concept, primarily based on information warfare and non-military means, linked to social conditions.

Fifth Period of Operational Art

Traditionally, operational art links to strategy as it develops campaigns and operations to organize and employ military forces by integrating ends, ways, and means to achieve the strategic end state.[57] The Chief of the General Staff of the Armed Forces, General Valerii Gerasimov, described the framework of the current Russian operational concept as the "[r]ole of Non-Military Methods in the Resolution of Interstate Conflicts."[58] Figure 2 depicts the operational framework divided in six phases: (1) concealed origin; (2) escalation; (3) outbreak of conflict activity; (4) crisis; (5) resolution; and (6) restoration of peace. The figure shows that traditional military actions are just a small part of the operational art. The phases before the conflict shape the end-state, not the military action itself.

The non-military lines of effort include: (1) creating and maintaining a military and political opposition; (2) economic and political pressure by sanctions, blockades and break in

---

[55] Marcel H. Van Herpen, *Putin's War: The Rise of Russia's New Imperialism* (Lanham, MD: Rowman and Littlefield, 2014), 47-62.

[56] Bertil Nygren, *The Rebuilding of Greater Russia: Putin's Foreign Policy towards the CIS Countries* (Abingdon, UK: Routledge, 2008), 219-250.

[57] Army Doctrine Reference Publication (ADRP) 3-0, *Unified Land Operations* (Washington, DC: Department of the Army, 2011), 4-2; JP 5-0, III-1.

[58] Gerasimov.

political relations; (3) formation of coalitions and alliances; and (4) finding ways to settle the conflict. Figure 2 shows the use of information warfare, combining military and non-military means, as a line of effort through all phases. Information warfare includes the use of technology, such as communications and the Internet, and psychology, which deals with influence of humans.[59] The strategic deployment of troops as a threat or intervention takes place during the crisis and resolution stage. Finally, deployment of peacekeeping forces to restore the *status quo* is another line of effort.

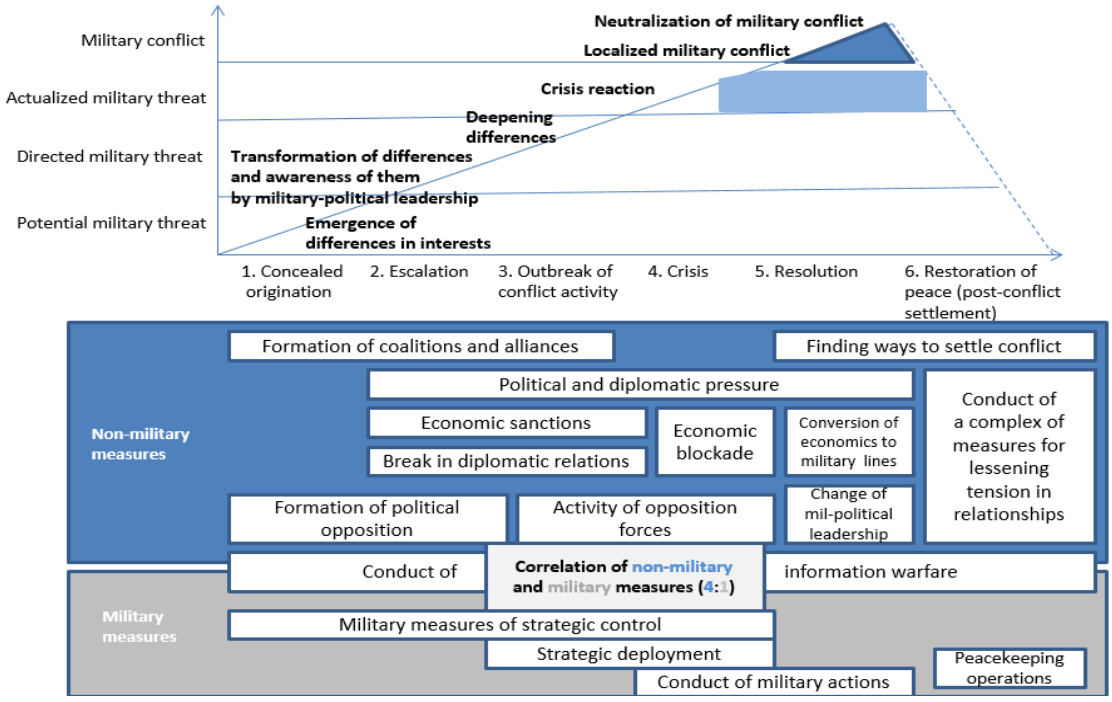

Figure 2. The Role of Non-Military Methods in the Resolution of Interstate Conflicts.

Source: Valery Gerasimov, "The value of science in anticipation," *VPK news*, 27 February 2014, accessed 2 July 2014, http://www.vpk-news.ru/articles/14632. Translated and created by Dr. G. Scott Gorman, School of Advanced Military Studies.

[59] John Bolen, "Operational Art goes Digital," *New Horizons* 7, no. 1 (April 2013): 30.

Gerasimov describes the new operational concept with some of the same principles as Georgii Isserson, a leading Soviet military thinker before World War II, did some 60 years ago. Isserson described operational art as the art of direction and organization in which operations are a chain of efforts throughout the entire depth of the operation's area, with principles of speed, efficiency, mobility, simultaneity, technological support, and a decisive moment at the final stage.[60] Gerasimov added to this operational concept the application of asymmetric and indirect actions by hybrid forces, military-civilian components, special forces, and technical weapons to weaken the economy and destroy key infrastructure.[61] The new operational concept thus is a continuation of the Russian operational art with different means in more domains, of which Russian and European defense experts tried to reveal the *modus operandi*.

These experts state that in the first phase, unconventional operations manipulate public opinion at home and abroad, while in the second phase disguised Russian forces aid the opposition. "New-generation war will be dominated by information and psychological warfare and asymmetric actions, to be used extensively to level off the enemy's superiority in armed struggle."[62] Diplomats, media, and interagency organizations conduct deception operations and leak false data, orders, and directives, in order to misinform and mislead the enemy's political and military leaders. At the same time, cyber-attacks must disable other media or communication systems in the enemy's country to prevent him from gaining information. In the two opening phases, this concept encompasses the use of communication and psychology, based on social

---

[60] Georgii S. Isserson, "The Evolution of Operational Art," trans. Bruce W. Menning (Fort Leavenworth, KS: SAMS Theoretical Special Edition, 2005), 38-77.

[61] Gerasimov.

[62] Sergey G. Chekinov, and Sergey A. Bogdanov, "The Nature and Content of a New-Generation War," *Voyennaya Mysl* 10, no. 4 (2013): 13-24.

conditions. In these phases, Russia uses SOF, space, electronic, diplomatic, and industrial means to map key infrastructure in the targeted area and conduct subversive missions.[63]

The third phase encompasses unconventional operations with the help of proxy forces to destroy or take over key infrastructure. These actions either provoke a conventional response by the enemy or establish a *status quo*. These proxy forces are most likely ethnic Russians that benefit from a Russian intervention. A conventional answer by the enemy leads to intervention by overwhelming RFAF conventional forces to seize the targeted area and reach the desired operational end state. In this third and the following fourth phase, all actions must contribute to a cumulative effect on the enemy leadership to ensure they are unable to resist the RFAF anymore and are willing to negotiate a diplomatic settlement. Finally, in the fourth and fifth phase, the RFAF sends peacekeepers to the area, using the protection of ethnic Russians as justification.[64] Parts of the operational concept must affect human psyche, moods, and will, and together with mass-scale propaganda, create chaos and loss of control to the point that the enemy feels so confused and experiences such despair that it leads to paralysis of the country's leadership.[65]

Theory on previous periods of Soviet and Russian operational art reveal how operational concepts effect the human psyche, moods, and will by a systems approach: military systemology. Military systemology is an intellectual-informational confrontation that seeks to dominate and

---

[63] Chekinov and Bogdanov: 13-24.

[64] Ibid.

[65] Bugajski, "The Shadow War," *Central Europe Digist* (9 May 2014), 2; Jānis Bērziņš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* (Riga, National Defense Academy of Latvia, Center for Security and Strategic Research: 2014), 6.

gain strategic initiative from the beginning.[66] In this systems approach, operational shock must lead to the disruption of the enemy capability and system to command and control its forces.[67] The RFAF thoroughly analyzes its enemy, the characteristics and weaknesses of its command and control system, and its willingness to fight, in order to arrange interdependent sequential mechanisms that deteriorate parts of the enemy command and control system and degrade the enemy's willingness to fight. Russian operational art is more than planning for offensive operations; it has been since long before 2000 a systems approach based on psychology.[68]

The Soviet Army used military systemology in the 1970s to conduct reflexive control as a mean of psychological warfare.[69] Reflexive control is "[a] mean that provides military commanders with the ability to indirectly maintain control over his opponent commander's decision process."[70] With reflexive control, the military persuades the enemy to take favorable actions by altering information available to him in order to deceive, tempt, intimidate, or disinform him.[71] It uses the enemy's cultural, ethnic, historical, language, and behavior background to insert new information at a preplanned moment. Reflexive control uses predefined

---

[66] Kipp, "Operational Art and the Curious Narrative on the Russian Contribution: Presence and Absence Over the Last 2 Decades," in *The Russian Military Today and Tomorrow - Putin, Russian Navy, Ukraine, Gazprom, Rosneft, Lavrov, Deep Operations, Campaign Design, Russian-Chinese Security Relations, Mafia and Arms Dealers*, eds. Stephen J. Blank and Richard Weitz (Carlisle PA: Strategic Studies Institute, U.S. Army, 2014), 3110-3112, Kindle ed.

[67] Simon Naveh, *In Pursuit of Military Excellence: The Evolution of Operational Theory* (Abingdon, UK: Frank Cass Publishers, 1997), 11-19.

[68] Thierry Gongora and Harald Von Riekhoff, *Toward a Revolution in Military Affairs? Defense and Security at the Dawn of the Twenty-First Century* (Santa Barbara, CA: Greenwood Publishing Group: 2000), 96; Kipp, "Operational Art and the Curious Narrative on the Russian Contribution," 3016-3017, Kindle ed.

[69] Gongorra and Von Riekhoff, 96.

[70] Clifford Reid, "Reflexive Control in Soviet Military Planning," in *Soviet Strategic Deception*, ed. Brian Dailey and Patrick Parker (Stanford, CA: The Hoover Institution Press, 1987), 294.

[71] Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness* (Fort Leavenworth, KS: Foreign Military Studies Office, 2011), 124-126.

mechanisms that, as depicted in Table 1, apply military and non-military ways and means depending on the enemy's background and the desired effect.

Table 1. Mechanisms of Reflexive Control	
Deception	forcing the enemy to reallocate forces to a threatened region during the preparatory stages of combat operations
Deterrence	creating the perception of insurmountable Superiority
Distraction	creating a real or imaginary threat to one of the enemy's most vital locations during the preparatory stages of combat operations, thereby forcing him to reconsider the wisdom of his decisions to operate along this or that axis
Division	convincing the enemy that he must operate in opposition to coalition interests
Exhaustion	compelling the enemy to carry out useless operations, thereby entering combat with reduced resources
Overload	frequently sending the enemy a large amount of conflicting information
Pacification	leading the enemy to believe that pre-planned operational training is occurring rather than offensive preparations, thus reducing his vigilance
Paralysis	creating the perception of a specific threat to a vital interest or weak spot
Pressure	offering information that discredits the government in the eyes of its population
Provocation	force him into taking action advantageous to your side
Suggestion	offering information that affects the enemy legally, morally, ideologically, or in other areas

Source: Created by author, based on Timothy L. Thomas, *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness* (Fort Leavenworth, KS: Foreign Military Studies Office, 2011), 129-130.

Finally, Russian operational art relies on concealment, also a technique of reflexive control, divided in two levels. Operational level concealment are "[t]hose measures to achieve operational surprise and is designed to disorient the enemy regarding the nature, concept, scale, and timing of impending combat operations."[72] Strategic level concealment are "[t]he activities that surreptitiously prepare a strategic operation or campaign to disorient the enemy regarding the true intentions of actions."

From the previous paragraphs, it becomes clear that Russian operational art has made a shift in means and domains. It serves the near-abroad policy by the use of non-military means in

[72] Thomas, *Recasting the Red Star,* 107-108.

non-traditional domains, based on social conditions. The operational art's primary tenets, principles, and systems approach based on reflexive control and concealment, remain the same as in previous periods of Russian operational art.

Section 2

Russian Operational Art in Practice

> A critical inquiry –the examination of the means– poses the question as to what are the peculiar effects of the means employed, and whether these effects conform to the intention with which they were used.
>
> —Carl Von Clausewitz, *On War*

This second section explores how Russia applied its new operational concept during the Estonia, Georgia, and Ukraine conflicts and provides insights to construct a recognizable operational framework in the next section. As a lens, each case study uses the preliminary operational framework as sketched in the previous section, focusing on non-military means, social conditions, and achieved effects.

2007 Estonia Case Study

Estonia became independent from the USSR in March 1991. At that time, the Estonian government passed a law that rejected Russian as an official language, forcing the Estonian language on ethnic Russians as a requirement to earn Estonian nationality.[73] Russia saw this as a marginalization of the rights of 1.3 million ethnic Russians, some twenty-five percent of the Estonian population. Many of these ethnic Russians lived in the Narva region next to the Russian border, but did not claim to belong to Russia out of fear of a "Moldova war."[74] Tensions increased as Estonia joined the EU and NATO in 2004 and subsequently refused to let Russia

[73] Claus Neukirch, *Russia and the OSCE- The Influence of Interested Third and Disinterested Fourth Parties on the Conflicts in Estonia and Moldova* (Flensburg, Germany: Centre for OSCE Research, 2001), 8.

[74] Ibid., 9-10.

build a pipeline through its waters to Germany.[75] The event that sparked the Russia-Estonia crisis of April 2007 was the relocation of the Bronze Soldier, a memorial to commemorate the Soviet liberation of Estonia from Nazi Germany, from central-Tallinn to a neighboring cemetery.

The escalation phase started with violent riots in Estonia and demonstrations at the Estonian embassy in Moscow as ethnic Russians saw the movement of the Bronze Soldier as a further marginalization of their rights in Estonia.[76] A Russian youth group named *Nashi* [Ours], aided by Russian SOF, organized riots in Russia and Estonia.[77] Assisted by Russian media, the rioters in Moscow and Tallinn protested for the human rights of ethnic Russians in Estonia, often comparing the ethnic Estonians with the Nazis of World War II.[78] Russia started issuing passports to ethnic Russians and pushed the Estonia government to make Russian the second national language and an official language of the EU.[79]

The outbreak of the conflict activity phase started with cyber-attacks that occurred in two waves. The cyber-attack on 27 April 2007 was a spontaneous, uncoordinated attack on government, financial, economic, news, and military networks.[80] Through media and Internet groups, Russian sympathizers encouraged Russians around the world to join the attacks and to download software to establish a worldwide network of supporting computers.[81] *Nashi* openly

---

[75] Vladimir Socor, "Nord Stream Project: Bilateral Russo-German, Not European," *Eusasia Daily Monitor* 4, no. 179 (2007), accessed 1 September 2009, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=33033&no_cache=1#.VAUMVsVdW_s.

[76] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 50-51.

[77] Max G. Manwaring, *The Complexity of Modern Asymmetric Warfare* (Norman, OK: University of Oklahoma Press, 2012), 91.

[78] Van Herpen, 130.

[79] Michael J. Williams, "Tomorrow's War Today," *Central Europe Digist* (May 2014): 9.

[80] Heickero, 39.

[81] Scott J. Shackelford, "Estonia Three Years Later: A Progress Report on Combating Cyber Attacks," *Journal of Internet Law* (February 2010): 22.

joined the cyber-attacks, which faded away after a few days.[82] The second attack, 8 May 2007, was more sophisticated and overwhelmed the government, financial, economic, news, and military websites and networks.[83] The attack coincided with the anniversary of the Soviet victory over Nazi Germany, an event used by Russian sympathizers to stir up discontent. The second attack denied targeted institutions use of their websites, disabled phone communication, and disrupted the government's email server, effectively hampering the government's ability to lead the country and communicate with its allies.[84] The EU at this time did not react due to internal discussion on the crisis. Russia thus isolated the Estonian government for a few days from its country, allies, and armed forces.

At this point, the conflict shifted very fast into the crisis and resolution phases. Russia tried to put the Estonian government under additional pressure by threatening to reduce gas delivery. Despite the short period of isolation and the fact that Russia was the sole supplier of natural gas to Estonia, it was unable to pressure Estonia into a settlement on the statue and language issues, although Estonia did move the statue to a more prominent location then previously planned.[85] The impact of the attacks on Estonia and its economic, military, and financial institutes was minimal and of short duration.[86] The crisis, however, verified Russian doctrine on cyber warfare, targeting populations, financial and economic institutions, intelligence services, and all levels of government as an aid to temporarily disorient and cripple

---

[82] Van Herpen, 130.

[83] Ibid.

[84] Heickero, 39.

[85] Bradley L. Boyd, "Cyber Warfare: Armageddon in a Teacup?" (Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2009), 35.

[86] IHS Jane's, 9.

governments.[87] Russia also found a way to attack in a domain that had no legal counter actions; Estonia could not approach the United Nations or NATO allies, as these institutions do not consider cyber-attacks by individuals as state on state warfare.[88] As of this writing, the language issue remains unsolved.

2008 Georgia Case Study

Georgia became independent from the USSR in 1991and tensions started immediately over two breakaway regions: South Ossetia and Abkhazia. These regions wanted to remain within the USSR due to their troubling history with Georgia. After two short civil wars, both regions established internationally unrecognized pro-Russian local governments, while Georgia had to accept Russian peacekeeping forces in these areas.[89] South Ossetia and Abkhazia did not have large ethnic Russian populations, but the inhabitants had a distinctly different culture and language than Georgia, more related to the areas north of them, inside Russia.[90] Over the following years, Russia issued Russian passports to the inhabitants of the breakaway regions and thus created a Russian minority it promised to protect.[91] The rising tensions with Georgia were a

[87] Heickero, 22.

[88] Cassandra M. Kirsch, "Science Fiction No More: Cyber Warfare and the United States," *Denver Journal of International Law and Policy* 40 (2012): 630-634.

[89] David Hollis. "Cyberwar Case Study: Georgia 2008," *Small Wars Journal,*, 6 January 2011, accessed 7 September 2014, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008; Cohen and Hamilton, 4.

[90] Advameg, Inc. "Georgia," Countries and their Cultures database, accessed 7 September 2014, http://www.everyculture.com/Ge-It/Georgia.html#ixzz3CHXlfxMG.

[91] Janusz Bugajski, "Georgia: Epicenter of Strategic Confrontation," *Centre for Strategic & International Studies (CSIS)*, 12 August 2008; De Haas, "Russia's Military Doctrine Development (2000-2010)," 46; Cohen and Hamilton, 5.

result of the Russia's fear of NATO expansion and the desire for a regime change in Georgia.[92] The latter was a reaction to Georgia's harboring and supporting Chechen separatists' groups.

During the escalation phase, early 2008, Russia sent railway troops into Abkhazia to repair railroad infrastructure under the peacekeeping agreement.[93] Russia covertly raised the number of peacekeeping troops by moving several hundred elite paratroopers disguised as peacekeepers in the region.[94] Finally, the RFAF conducted an exercise near the border of Georgia in July, enabling rehearsals for an invasion.[95] Russia stepped up its information warfare campaign during the escalation phase and continued it during the outbreak of conflict and crisis phases.[96] During these three phases, the media targeted multiple audiences with several aims.

First, it targeted Russian and breakaway region inhabitants, appealing to their patriotism, justifying the cause of an eventual intervention, and convincing them to join cyber, proxy, or partisan forces. The media campaign used Georgian support to Nazi Germany to demonize the country and its government in the eyes of Russians.[97] The *Nashi* youth group again supported this campaign.[98] Second, media targeted the international community, projecting a "Kosovo" scenario on the situation in Georgia based on discrimination of and atrocities against ethnic Russians by Georgia.[99] Russia justified its intervention in this way. Third, media targeted the population of

---

[92] Van Herpen, 233-234.

[93] Cohen and Hamilton, 18.

[94] George T. Donovan, "Russian Operational Art in the Russo-Georgian War of 2008" (Strategy Research, US Army War College, Carlisle Barracks, PA, 2009), 9-10.

[95] Cohen and Hamilton, 19.

[96] Mattsson and Eklund, 34.

[97] Websites such as http://4international.me/2008/08/09/georgia-neo-nazi-war-against-ossetia-has-begun/ use the link between Nazi past and present situation.

[98] Manwaring, 92.

[99] Jadwiga Rogoza and Agata Dubas, "Russian Propaganda War: Media as a Long – and Short-range Weapon," *Centre of Eastern Studies Commentary*, no. 9 (11 September 2008): 2-3.

Georgia to discredit its government and set stage for the abolition of the government. Final, information warfare targeted the Georgian government and military leadership, in the outbreak of conflict and crisis phases joined by cyber-attacks, to isolate them.

With cyber-attacks on NATO, Georgian government, media, and military networks, the conflict shifted to the outbreak of conflict phase.[100] The cyber-attacks were unsophisticated disruptive attacks, not designed to penetrate the networks and misuse them, but to make the networks unusable.[101] Russian nationalists and *Nashi* joined the cyber-attack for which pro-Russia websites provided the software ready to download.[102] These cyber-warriors infected many other computers that could participate in distributed denial of service attacks. At this point, the cyber-attacks hampered the Georgian government's ability to communicate with the world.

The Russian information warfare campaign is a clear example of reflexive control to shape perceptions prior to military operations in South-Ossetia and Abkhazia. Russia used proven media techniques: (1) one-sidedness of information; (2) information blockade; (3) disinformation; (4) silence over events inconvenient for Russia; (5) "cherry picking" of eyewitnesses and Georgians that criticized their government; (6) denial of collateral damage and (7) Russian versions of place names in the regions to suggest the motherland relation.[103] These techniques supported the reflexive control mechanisms of overload, pressure, and suggestion. Cyber-attacks

---

[100] US Cyber Consequences Unit (US-CCU), *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008* (Washington, DC: US-CCU, 2009), 2-6.

[101] IHS Jane's, 10.

[102] McAfee, *Virtual Criminology Report 2009* (Santa Clara, CA: McAfee, 2009), 6; Van Herpen, 130.

[103] Rogoza and Dubas: 3-4.

established the information blockade. These information warfare actions also attempted to provoke the Georgian government to take military action in the breakaway regions; it worked.[104]

The crisis phase started on 7 August 2008 with a Georgian attack on South-Ossetia, an action used by Russia justify its own intervention. With the help of media, Russia created an image of a deliberate and unprovoked Georgian attack on both breakaway regions, forcing Russia to intervene and prevent a genocide.[105] Cyber-attacks hampered the Georgian government's ability to govern its country, crippling army command and control systems, including air defense.[106] The RFAF invasion started during the Olympic Games in China to prevent an international focus on the war and delay an international reaction. The speed and success of the Russian campaign, together with the temporary inability to react, control, or inform, made it impossible for the Georgian government to counter Russian messaging. In order to justify the scale of the Russian invasion, Russian media and leadership exaggerated the Georgian military invasion.[107] Russia also used embedded journalists to deliver the evidence of Russian minority oppression and ethnic cleansing while preventing the Georgian government from countering these stories through use of information warfare and cyber.[108]

Russian peacekeepers, local proxy forces, and Cossack units that answered the media call joined the regular RFAF fight.[109] Furthermore, the RFAF dropped forces in unmarked uniforms

---

[104] Nathan D. Ginos, "The Securitization of Russian Strategic Communication" (Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2010), 11.

[105] Mattsson and Eklund, 35.

[106] US-CCU, 2-6.

[107] Donovan, 11-12.

[108] Mattsson and Eklund, 35; Hollis.

[109] Donovan, 14; Daily News Bulletin, "Cossack Volunteers to Help South Ossetia," *Daily News Bulletin* 8, English ed. (August 2008).

behind Georgian lines to conduct subversive actions.[110] Overwhelmed by force and simultaneous, in-depth actions, together with the disruption of their situational awareness and communications, Georgian commanders were psychologically put on the defensive.[111] The Russian operational objective was to secure the breakaway regions. Once secured, the RFAF pushed on in support of other efforts, the navy blockaded the coast while the army seized transportation infrastructure and threatened the pipelines to degrade the economy.[112]

Shifting towards the resolution phase, Russia stopped short of Tbilisi and international oil pipelines to avoid an international reaction. Isolated from the outside world and with a large part of Georgia occupied by Russia, the Georgian government became willing to negotiate peace terms. After ensuring their operational objectives, RFAF withdrew on 12 August into South-Ossetia and Abkhazia.[113] The results of the conflict caused NATO to reconsider its offer of membership to Georgia and Russia unilaterally recognized the independence of the separatist republics Abkhazia and South-Ossetia.[114] Russia's strategic objective was halting NATO's expansion, warning other former Soviet states not to pursue NATO membership.[115] The conflict remains frozen as of this writing.

2014 Ukraine Case Study

Ukraine became independent of the USSR in 1991 and tensions soon followed, largely because of an ethnic Russian minority in Crimea that wished to join Russia. In their support, and

---

[110] Cohen and Hamilton, 42.

[111] Mattsson and Eklund, 34.

[112] Donovan, 8-16.

[113] Ibid., 7.

[114] Mattsson and Eklund, 34; Donovan, 1.

[115] Donovan, 6; Bugajski, "Georgia: Epicenter of Strategic Confrontation."

to influence Ukraine and international perception, the Russian government emphasized that the majority of the Crimean population were ethnic Russians, that this majority was reluctant to be part of Ukraine, and that Crimea was part of Russia between 1783 and 1954.[116] Tensions remained after Crimea became a Republic within Ukraine in 1998, with its own parliament because Ukrainian became the national language.[117] Pro-Russian attitudes remained as separatists groups stepped up their efforts, helped by the Crimean parliament that at this time was pro-Russian. Anti-Russia and anti-Western feelings in Ukraine would spark uprisings for the next fifteen years: the 2003 Orange revolution, 2008 Crimea unrest, and 2013 Euromaidan revolution.

The 2003 Orange revolution started after what many West-Ukrainians saw as corrupt elections, won by an East-Ukraine supported pro-Russian party.[118] The Orange revolution reversed the election outcome and ensured a more representative government. More importantly, it revealed that tensions not only involved Crimea, but also existed between pro-West and pro-Russian Ukrainians. In 2008, the Ukrainian government suppressed rallies in Crimea that were calling for a union between Ukraine and Russia.[119] Russia reacted by issuing Russian citizenship to ethnic Russians in Crimea.[120] In 2013, tensions between pro-Russian and pro-West sympathizers resulted in the Euromaidan revolution, sparked by an oil deal between ruling

---

[116] Victor Zaborsky, "Crimea and the Black Sea Fleet in Russian-Ukrainian Relations" **(**Discussion Paper 95-11, Harvard University, Cambridge, MA, 1995), 26.

[117] Igor Davydov, "The Crimean Tatars and their Influence on the "Triangle of Conflict" **—** Russia-Crimea-Ukraine" (Paper, Naval Postgraduade School, Monterey, CA, 2008), 39-43.

[118] Andrew Wilson, *The Ukrainians, Unexpected Nation* (London, UK: Yale University Press, 2009), 319-322.

[119] Davydov, 39-43.

[120] Zaborsky, 37.

President Viktor Yanukovych and Russia.[121] Riots started as pro-Western Ukrainians saw this as a move to reestablish stronger ties to Russia.

The escalation phase of the most current crisis started after President Yanukovych of Ukraine fled the country in February 2014 and a pro-Western government assumed power.[122] Russia argued that this was an illegal act as Ukrainians had not followed the impeachment procedure as depicted in Ukrainian law.[123] According to Russia, the new government acted against the security of Russians within Ukraine. Russia then used its policy of protecting Russians abroad to justify an intervention, again with reference to the Kosovo crisis.[124] Probably, the real strategic objectives were to halt NATO expansion and remain in control of the Crimean naval base, needed for all-year access to connecting seas and oceans.

Next was the media campaign to gain support in Crimea, Russia, and isolate the government of Ukraine. Television and Internet were the dominant news media in Ukraine.[125] The television channels in Crimea, from which some 95% of the population gathered their news, were Russian state owned. Some 50% gathered their news from the Internet. Furthermore, some 70% of the population of Crimea used the two major Russian social network sites available. Russia and Ukraine analyzed information on sentiments gathered from the Internet, finding a 76% score for pro-Russian sentiments in the region. In Russia itself, these figures were comparable. In

---

[121] Nadia Diuk, "EuroEuromaidan: Ukraine's Self-Organizing Revolution," *World Affairs*, April 2014, accessed 27 January 2015, http://www.worldaffairsjournal.org/article/euroEuromaidan-ukraine%E2%80%99s-self-organizing-revolution.

[122] Steven Woehrel, *Ukraine: Current Issues and U.S. Policy* (Washington, DC: Congressional Research Service, 2014), 1; Bērziņš, 2-3.

[123] Bērziņš, 2-3.

[124] Ibid.

[125] Gallup, *Contemporary Media Use in Ukraine* (Washington DC: Broadcasting Board of Governors, 2014), 1-2.

Russia, 75% of the population thought state owned media were trustworthy. Independent news providers rated as 30% trustworthy while outside news providers rated 5% reliable.[126] Russia thus established information dominance in the escalation phase.

Developments in the information sphere aided this dominance. In 2010, Russia established social media-groups such as the Kremlin School of Bloggers to support their reflexive control mechanisms.[127] Through a network of oligarchs, such as *Gazprom* Media, the Russian government acquired significant stakes in Russian and former Soviet states' social media, dating, blogging and other websites. [128] Control over popular websites, together with a 2008 law that gave Russia legal means to shut down any mass media websites that could influence the public negatively, created control over messaging through Internet comparable to TV and radio. This Russian law defined mass media as "[a]ny regularly updated Internet site can be included in the understanding of mass media, including personal diaries, various forums, and chats including."[129]

The information campaign started with the comparison of the Ukrainian government and their Western allies to Nazis, gays, Jews, and other groups of people that Russia claimed were part of the conspiracy.[130] It used Swastikas on billboards and in the media to compare the government to Nazi Germany. This would remain the case throughout the conflict. In addition, Russia's story since roughly 2008 is based on Russian Empire history as told by popular

---

[126] Julie Ray and Neli Esipova, "Russians Rely on State Media for News of Ukraine, Crimea. Few trust Western media or independent Russian media," *Gallup World*, July 2014, accessed 4 October 2014, http://www.gallup.com/poll/174086/russians-rely-state-media-news-ukraine-crimea.aspx.

[127] Van Herpen, 130.

[128] Central Intelligence Agency (CIA), "Kremlin Allies' Expanding Control of Runet Provokes Only Limited Opposition," *Media Aid* (28 February 2010): 1-5.

[129] CIA: 1-5.

[130] Alan Yuhas, "Russian Propaganda over Crimea and the Ukraine: How Does it Work?" *The Guardian*, 17 March 2014, accessed 4 October 2014, http://www.theguardian.com/world/2014/mar/17/crimea-crisis-russia-propaganda-media.

nineteenth century writer Fyodor Dostoevsky. He claimed, "Russia's special mission in the world was to create a pan-Slavic Christian empire with Russia at its helm."[131] Putin quotes the writer often, together with hints towards a Dostoevsky Russia in his speeches. Russia also used Western media as they oversimplified maps signifying east and south Ukraine as predominant Russian ethnic. The diplomatic channels and Russian leadership now started to emphasize the same issues of marginalized Russian minorities that seek reunification with Russia.

To prevent NATO and the EU from helping Ukraine, Russia stepped up its information campaign. Russian media used past events to emphasize how aggressive NATO and the West were and how these powers violated agreements on NATO expansion restrictions into Eastern Europe.[132] Furthermore, to shape the EU's perception of Ukraine as an unreliable partner, Russia made many public statements of Ukrainian violations of the Russian-Ukrainian agreement on revenue and energy rights related to the gas pipeline transiting Ukraine.[133] This further softened the already divided EU's response, resulting in a temporary isolation of Ukraine. Leaders of pro-Russian organizations gathered on 12 February to discuss Crimea's future and decided to support Russia.[134] The Russian Consulate in Crimea started issuing Russian passports to all inhabitants of the Crimea in the same week, to create a Russian majority on the peninsula. Finally, on 14

---

[131] Andrew Kaufman, "How Dostoevsky and Tolstoy Explain Putin's Politics," *Andrew D. Kaufman,* 7 April 2014, accessed 24/11/2014, http://andrewdkaufman.com/2014/04/dostoevsky-tolstoy-explain-putins-politics/.

[132] Dmitry Babich, "Media wars around Crimea: Russia not impressed by liars' empty threats," *The Voice of Russia,* 20 March 2014, accessed 4 October 2014, http://voiceofrussia.com/2014_03_20/Russia-not-impressed-by-liars-empty-threats-1813/.

[133] Ginos, 11.

[134] Robert Coalson, "Pro-Russian Separatism Rises In Crimea As Ukraine's Crisis Unfolds," *Radio Free Europe,* 18 February 2014, accessed 24/11/2014, http://www.rferl.org/content/ukraine-crimea-rising-separatism/25268303.html.

February, a cyber-attack took place targeting one of Ukraine's largest banks by malware, to support the unrest in the country.[135]

The outbreak of the conflict activity phase started on 27 February. Local paramilitary forces and Cossacks stormed the parliament and replaced it with pro-Russians, led by Sergei Aksyonov.[136] While pro-Russian sympathizers seized more key installations in Crimea, volunteers from Russia came to their aid and 40,000 troops strong Russian Army started exercises at the Ukraine-Russian border.[137] In the days after the seizure, Cossacks remained to protect the parliament buildings against the Ukrainian army or pro-Ukraine sympathizers. Though Russia denied involvement, Russian-speaking militants in unmarked uniforms occupied military airfield installations as of 28 February.[138] The militants further occupied the regional media and telecommunication centers and shut down telephone and Internet communication in Crimea as more planes with new troops landed at the seized airfields.[139]

More overt, the militants jammed radio and cellphone traffic to isolate Crimea further from Ukraine.[140] Cyber-attacks started at the beginning of March and targeted the Ukrainian

---

[135] IHS Jane's, 8.

[136] NOS, "Wie is de Baas op de Krim [Who is the Boss of the Crimea]," *NOS*, 11 March 2014, accessed 4 October 2014, http://nos.nl/artikel/622011-wie-is-de-baas-op-de-krim.html.

[137] Steven Woehrel, *Ukraine: Current Issues and U.S. Policy* (Washington, DC: Congressional Research Service, 2014), 1.

[138] NOS, "Militaire Spanning Krim Stijgt [Military Tension Crimea Rises]," *NOS*, 28 February 2014, accessed 4 October 2014, http://nos.nl/artikel/617230-militaire-spanning-krim-stijgt.html.

[139] NOS, "Kiev: Invasie door Russisch Leger [Kiev: Invasion by Russian Army]," *NOS*, 28 February 2014, accessed 4 October 2014, http://nos.nl/artikel/617425-kiev-invasie-door-russische-leger.html.; IHS Jane's, 8.

[140] IHS Jane's, 8.

government, as well as NATO websites.[141] Cyber-Berkut, a Ukrainian group that may possess ties to the Russian intelligence services, hosted the attacks. These attacks hampered NATO and Ukrainian leadership but did not lead to isolation or overload. The United States of America called for a UN mission in the region in March; Russia declined.[142] Instead, Prime Minister Aksyonov of the autonomous Republic of Crimea, together with former Ukrainian President Yanukovych, called for Russian intervention on 1 March and an independence referendum on 30 March.[143]

The crisis phase started on 7 March when paramilitary forces and Cossacks attacked Ukrainian military bases.[144] In some cases, Ukraine forces surrendered, while in others, the paramilitary forces and Cossacks had to use more force, supported by the militants, called "little green men" by Western media. These "green men" were well armed, well trained, wore uniforms and masks, and had no military emblems on their uniforms.[145] They would not talk to the media nor reveal their identity. While Russia commented on many events in the conflict it was consistently silent over events inconvenient for Russia, namely on the presence, or not, of

---

[141] Adrian Croft and Peter Apps, "NATO websites hit in cyber attack linked to Crimea tension," *Reuters,* 16 March 2014, accessed 4 October 2014, http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316; Russel Brandom, "Cyberattacks Spiked as Russia Annexed Crimea," *The Verge,* 29 May 2014, accessed 4 October 2014, http://www.theverge.com/2014/5/29/5759138/malware-activity-spiked-as-russia-annexed-crimea.

[142] NOS, "Internationale Missie Oekraine [International Mission Ukraine]," *NOS,* 1 March 2014, accessed 4 October 2014, http://nos.nl/artikel/617484-internationale-missie-oekraine.html.

[143] NOS, "Referendum autonomie Krim eerder [Crimean Autonomy Referendum Earlier]."

[144] NOS, "Russen Vallen Basis Krim Aan [Russians Attack Crimea Basis]," *NOS,* 7 March 2014, accessed 4 October 2014, http://nos.nl/artikel/620412-russen-vallen-basis-krim-aan.html.

[145] NOS, "Pro-Rusland-Campagne op Dreef [Pro-Russia-Campaign on a Roll]," *NOS,* 13 March 2014, accessed 4 October 2014, http://nos.nl/artikel/622506-proruslandcampagne-op-dreef.html.

Russian soldiers in Crimea.[146] With the government of Crimea removed by the separatists, the distraction, pressure, suggestion, and isolation mechanisms succeeded. The Ukrainian government at that point was not, and probably never was, the target for a physical isolation.

Next in the Russian approach were the tasks that would lead to either provocation or exhaustion and paralysis of the Ukrainian government. Although the Ukrainian government decided not to be provoked strategically, the result on the operational level was devastating. All actions combined lead to the breakdown of morale of the Ukrainian forces in Crimea, as they surrendered their 190 bases, in many cases to join Russian forces.[147] The "green men" isolated Ukrainian forces in their bases and then used the local Internet and media to start Military Information Support Operations, media campaigns, and intimidation in combination with bribery.[148] The militants had already cut the power lines on 2 March at the Ukrainian Navy's headquarter in Sevastopol, and followed this with the seizure of the Ukrainian Naval Forces communications facilities and sabotage of all communication lines.[149] All this time, a covert cyber-attack by Russian sympathizers was absent. The reason might be that Crimea is a small area and had only one Internet hub, already in the hands of the unknown troops.

The government in Kiev admitted that local police and armed forces either were sympathizing with the uprising or had low morale, lack of professionalism, or were corrupt.[150] Next, Russian Agents had penetrated local intelligence and security forces. Together, the lack of communications and support to the bases led to tactical and eventual operational isolation of the Ukrainian forces in Crimea and to their perception of despair. On the other side, the "green men"

---

[146] Yuhas.

[147] Bērziņš, 4-5.

[148] Ibid.

[149] IHS Jane's, 8.

[150] Woehrel, 3.

remained disciplined in not revealing their identity and in not escalating the fight into a conventional war.[151] In April 2014, Russia admitted that the "green men" were in fact RFAF Spetznaz and Airborne troops.[152] On 16 March, Crimea held the referendum for independence earlier than planned and 96.77% voted for a reunification with Russia (turnout of 83.1%). The Russian Duma signed a treaty on 18 March formally incorporating Crimea into Russia. The conflict remains frozen as of this writing.

From the previous sub-sections, it becomes clear that Russian operations used non-military means linked to social conditions and reflexive control mechanisms for the preliminary operational framework as depicted in the first section. The ends, means, and ways together form the refined operational framework as depicted in the next section.

[151] Bērziņš, 4-5.

[152] Woehrel, 2; Bērziņš, 4.

Section 3

Russian Operational Framework

> Observe calmly; secure our position; cope with affairs calmly; hide our capacities and bide our time; be good at maintaining a low profile; and never claim leadership.
>
> —Deng Xiaoping, *24 Character Strategy*

This third section provides a synthesis of the previous sections' results. It describes the *modus operandi* of the current Russian operational framework, the use of non-military means, and exploitation of social conditions. This framework contains a schematic systems approach that Russia will use in future conflicts, with elements and means that vary per conflict, based on the environment and enemy.

Ends, Ways, and Means

The case studies show that Russian operational art serves the strategic goals of maintaining a sphere of influence in the near abroad, either by preventing former Soviet states from joining NATO or EU or destabilizing those states that already joined these alliances. As Russia sees itself in a continuous struggle with the West over influence in the former Soviet states, it has developed a tailored operational concept to reach its strategic ends. This operational concept creates conditions of instability within non-NATO countries so the alliance will not accept their membership. It also creates instability within NATO countries to keep the alliance fragile. Conflicts with Russia generally end up frozen, destined to start again when the opportunity arises. How these conflicts will emerge again is a question of time and inspiration on the Russian part.

The current Russian operational concept is a whole of systems, methods, and tasks to influence the perception and behavior of the enemy, population, and international community on all levels. It uses a systems approach based on reflexive control to target enemy leadership and alter their orientation in such a way that they make decisions favorable to Russia and take actions

that lead to a sense of despair within their leadership and establish a base for negotiation on Russian terms. Reflexive control "considers psychological characters of humans and involves intentional influence on their models of decision making."[153] With these characteristics, it reveals a cognitive model that reflects the internal structure of a decision-making system. This model delivers an approach of interrelated mechanisms based on history, social conditions, and linguistics to deceive, tempt, intimidate, or disinform. These reflexive control mechanisms are deception, deterrence, distraction, division, exhaustion, overload, pacification, paralysis, pressure, provocation, and suggestion; see Table 1. If one of these mechanisms fails, the overall reflexive control system must have an alternative route, or it might degrade quickly.[154]

To achieve the desired effects, Russia uses a mix of military and non-military means for speed, depth, simultaneity, shock, and concealment. Russia uses proxy forces, either paramilitary or cyber, and supports these forces with (media) institutions and companies, Spetsnaz, and Cossack fighters that together conduct unconventional warfare, information warfare, psychological operations, cyber warfare, security forces assistance, and strategic communication. Russia manages these military and non-military means through state controlled companies and organizations under a centralized political command structure. This structure, and the fact that the proxy forces consist of Russians and ethnic Russians abroad, make the operational concept a whole-of- society approach.

To create proxy forces, Russia exploits social conditions, culture, linguistics, and demography in former Soviet states and at home. It studies the behavior and demography of all actors to reveal cultural landmines or advantages it can exploit to achieve its objectives. Due to Russian policy in the Soviet-era, some 25 million Russians live in surrounding states where they

---

[153] Volodymyr N. Shemayev, "Cognitive Approach to Modeling Reflexive Control in Socio- Economic Systems," *Information and Security* 22 (2007): 35.

[154] Thomas, 131.

had better paid jobs than in Russia, either as civil servants, teachers, or in the military. Their new home countries marginalize their position through language legislation, rewriting national history, or limiting their civil rights, causing concerns in Russia with the Russian public and therefore Russian government. The Georgia and Ukraine case studies show that areas with a high concentration of ethnic Russians are vulnerable to Russian influence. In most cases, Russia will infuse the situation by granting citizenship to ethnic Russians or other inhabitants with grievances, creating Russian citizens in surrounding states that it is willing to protect.

First Phase: Concealed Origin

During planning in the first phase, Russia thoroughly analyzes his enemy, the characteristics and weaknesses of his command and control system, and his willingness to fight in order to arrange interdependent, sequential reflexive control mechanisms that can deteriorate parts of the command and control system and degrade the enemy's willingness to fight during the next phases. The case studies show Russia's narrative to intervene in neighboring countries is to protect Russian minorities. The region itself most likely contains a frozen conflict in which, after the decline of the USSR, groups of actors already showed their desire to join Russia. The reflexive control mechanism to justify this claim is distraction, the creation of an imaginary threat that Russia can use for justification and distract the targeted country and the international community from the real intent.

An ethnic Russian minority that wants support from Russia because it feels marginalized or mistreated by the current government is useful to create distraction. Russia influences actors in the region with the use of mass media to emphasize historical, cultural, and linguistic conditions, issues them Russian citizenship, and exploits these conditions to tempt them to take the Russian side. Russia establishes one-sidedness of information or information dominance in the enemy's country by buying local TV and radio stations, social media, and conducting influence operations on the Internet by blogger groups. Finally, the Russian minorities receive help from Russian

youth groups and the Russian Orthodox Church. After establishing these pre-conditions, the operational approach shifts to the next phase.

Second Phase: Escalation

In the escalation phase, Russia exploits the social conditions and information dominance to create social unrest. In this phase, Russia uses historical sentiments that will increase the unrest, such as support by the targeted country for Nazi Germany and Russia's destiny to be the major regional power based on the history of the Russian empire. Honor, patriotism, and dreams of a better future are strong elements to help actors' self-confidence and sense of self-worth, create involvement in social activity, develop community networks, and provide a forum to explore personal rights.[155] Ultimately, this model builds community organizations that want to contribute to the conflict resolution. These organizations get arms, training, and finance from Russian government-controlled organizations such as the National Bank, *Nashi*, Union of Cossacks, military units such as CIS peacekeeping forces (if present), and Spetsnaz. In the same way as Russia persuades ethnic Russians abroad to join the fight, it persuades Russians at home and abroad to join cyber-communities. These cyber-communities contribute to the fight by providing their assets (such as computers with Internet access) through downloading attack software. Special organizations set up for the occasion provide this attack-software.

In addition, in the beginning of the escalation phase, Russia targets the international community through media and diplomats on international legal matters, aided by legal deniability (e.g. not involved in the uprising, as part of concealment), stressing that the targeted government is suppressing a minority, including self-determination. The case studies show that Russia uses the Kosovo case where Western countries intervened to help the Kosovar minority to attain self-

---

[155] Yael, Ohana, *Supporting Cultural Actors of Change in Belarus, Moldova and Ukraine: A Regional Review* (Washington, DC: The German Marshall Fund of the United States, 2008), 9.

governance. Russia now claims this a precedent for it to intervene to help Russian minorities. By not claiming leadership, aided by the concealment of operations, Russia maneuvers between international laws, makes sure the targeted government does not get any outside support, and divides it from its allies or international support. Russia's uses a broad interpretation of United Nations Article 1 on internal conflicts and the right to self-determination to aid its approach.[156]

Next, Russia targets the population in the rest of the country and Russia to isolate the targeted government psychologically from its people and raise further support for intervention. With the reflexive control mechanism of pressure, it will try to convince the rest of the country that their government is not legal, is not in control, is not serving their interest, and will lead them in a useless war it cannot win legally nor militarily. To enhance this perception, cyber-attacks create financial market unrest by disrupting local banks. All this time, Russia operates under a blanket of concealment and legal deniability, preventing the international community from taking actions. The ethnic Russian minority then must create civil unrest and gradually seize key infrastructure in the targeted region, to start the next phase.

Third Phase: Outbreak of Conflict Activity

The third phase, outbreak of conflict activity, sees a difference between Russian interference in non-NATO and NATO countries. In both situations, Russia will increase its information warfare altogether with diplomatic and economic pressure and continue to create unrest. The Estonia case study shows that the Russian approach limits itself to these ways and means, while the Georgian and Ukrainian case studies reveal an additional approach.

In the latter, Russia uses a mixture of the organizations that are present, together with subversive elements such as SOF and Cossack fighters to seize key infrastructure. The enemy's

---

[156] United Nations (UN), *Charter of the United Nations* (New York, NY: United Nations, 1945), charter 1, article 1.

security forces in the targeted region probably contain local actors that are willing to join Russian organizations or at least not hamper these organizations in achieving their goals. At the same time, RFAF conducts large exercises at the border with the targeted country. These forces act in the beginning as pacifier, leading the enemy to believe that pre-planned operational training is occurring rather than offensive preparations, thus reducing his vigilance. At the end of the phase, these forces become the deterrence, creating the perception of a superior force that is able to intervene successfully. If this military approach succeeds and the targeted country does not react, Russia achieves its first operational goal; a part of the country is under control of separatists. Russia can exploit this fact politically to further establish its power in that region.

Fourth Phase: Crisis

In the crisis phase, Russia isolates the enemy government physically by rendering communication with their population, international community and media, and military leadership useless by directed electronic warfare and hard or soft cyber-attacks. In the case of soft cyber-attacks, overwhelming Internet attacks by Russian cyber-crime organizations and cyber proxy forces will reduce the government and military networks and phone systems in a manner that outmaneuvers applicable international laws. First, the cyber-attack means are not an "armed force" as Article 51 of the UN charter describes.[157] Second, although the UN can categorize the outcome of a cyber-attack as an "armed conflict," Russia makes sure that nobody can establish organizational and technical links to the cyber-attacks.[158]

In the case of hard cyber-attacks, proxy forces seize and disable or destroy physical Internet hubs, as was the case in the Ukrainian case study. This is part of the ongoing seizure of

---

[157] Titiriga Remus, "Cyber-attacks and International law of armed conflicts; a jus ad bellum perspective," *Journal of International Commercial Law and Technology* 8, no.3 (2013): 189-189.

[158] Remus; Cohen and Hamilton, 45.

infrastructure throughout this phase. Proxy forces, with the help of Spetsnaz and Cossacks fighters, will tighten their grip on the occupied area by removing areas of resistance, forcing isolated enemy units to surrender and seizing remaining government buildings. The Ukrainian case study reveals that if there are not enough proxy forces, Spetsnaz and Cossack fighters will do the majority of the work, making this phase less vulnerable to the cooperation or capabilities of the proxy forces.

In addition, Russia overloads the targeted government and population with information, suggesting that they cannot win the battle, their government is not legal, and that they are isolated from their allies and international community. Russia targets the military with misinformation on the whereabouts of the RFAF, actions, outcomes, etc., as part of the concealment and deception. The means are Russian media, RFAF Military Information Support Operations capacity, and the already mentioned cyber-attacks. These actions pressure, disorient, and overload the political and military leadership, which will lead them to taking the wrong actions, and even might provoke them to react militarily. If the latter happens, Russia will use its deterrence force to counter-attack.

Although the Russian conventional force is superior and victory is almost certain, this is an undesired escalation as Russia seeks a psychological victory, not a physical one. Rather than military action, Russia wants to let the reflexive control system take its effects, as the culminating effect of its mechanisms of disorientation, overload, pressure, suggestion, pacification, deterrence, deception, and concealment must overcome the provocation and cause the political and military leadership to exhaustion, paralysis, and a perception of despair. This perception sets the leadership up for the resolution phase.

Fifth and Sixth Phase: Resolution and Restoration of Peace

In the resolution phase, Russian diplomats step in to negotiate favorable terms to settle the conflict or to freeze it for future options. All case studies have an indefinite ending: language

and historical issues remain, while civil rights do not improve. Although Russian diplomats emphasize these issues during the peace settlement, they probably do not want to solve them. Solutions would degrade the elements of the pretext of Russian operational art by removing grievances that Russia needs to mobilize proxy forces in the next conflict. The Georgian conflict ended with independent regions, guarded by CIS peacekeeping forces, just as the Moldovan conflict fifteen years before. The annexation of Crimea thus far has resulted in an occupation by RFAF. These are the options Russia has for non-NATO countries. The end state for the Estonia crisis is different, as Estonia did not see a military uprising nor Russian intervention. Estonia did move the statue of the Bronze Soldier statue to a more prominent location though, giving in to Russian pressure.

The case studies reveal that Russia achieved it strategic goals: preventing non-NATO countries from joining NATO and destabilizing a NATO country to pressure it into a settlement. After the Georgian conflict, leading RFAF generals stated that they started planning the Georgia operation three months before the conflict, an indication that it was not a reaction on Georgia but a planned operation.[159] Although there are no indicators that this is the case in Estonia and Ukraine, Russia sees itself in a constant struggle with the West, and therefore probably plans contingencies for operations in the near abroad, after the restoration of peace.

To conclude, figure 3 depicts the Russian operational framework by phase with tactical tasks related to non-military means, in which ways and ends relate to the reflexive control mechanisms.

[159] Van Herpen, 219.

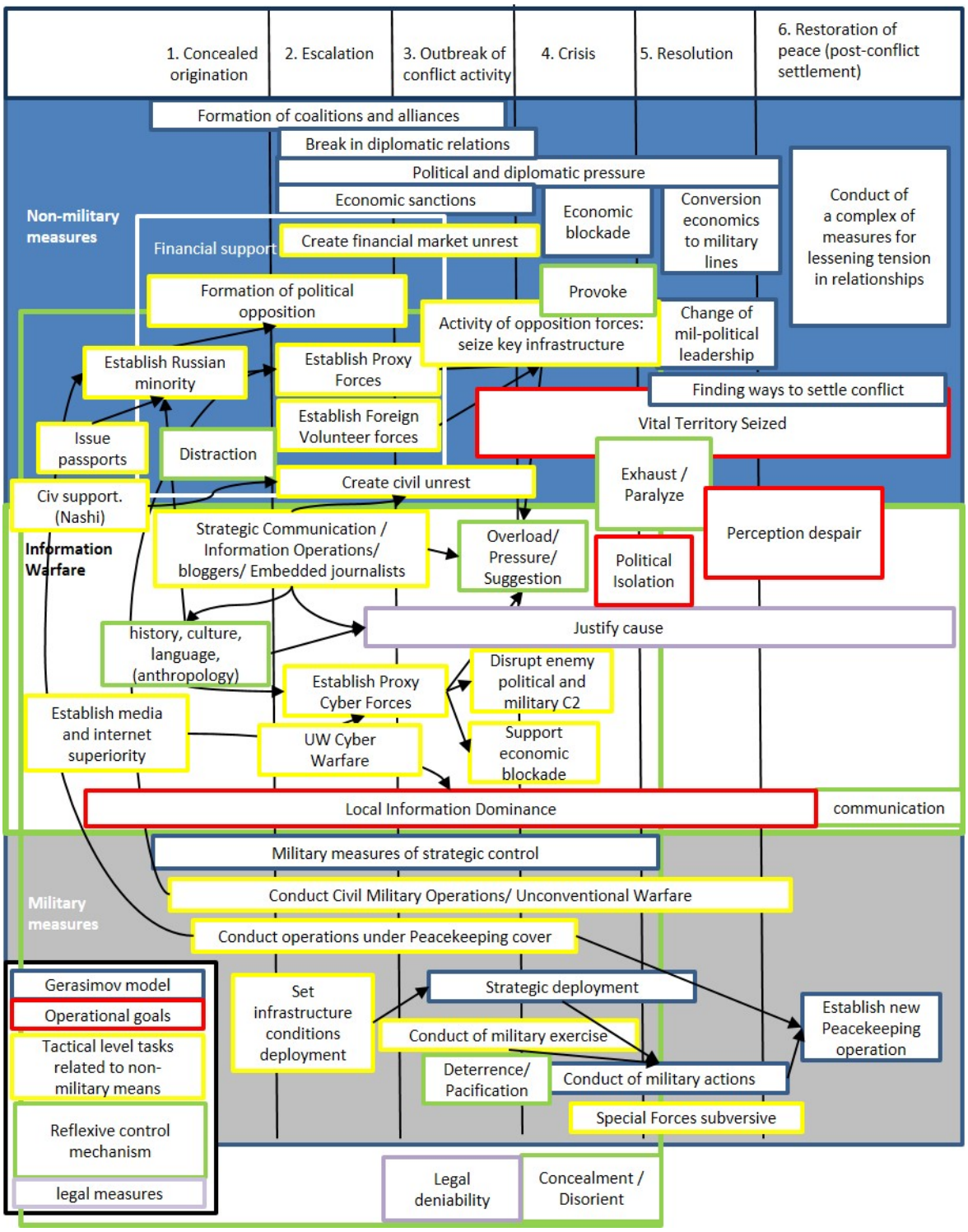

Figure 3. Generic Russian Operational Framework

Source: Created by author, based on Valery Gerasimov, *"The value of science in anticipation,"* VPK news, *27 February 2014, accessed 2 July 2014, http://www.vpk-news.ru/articles/14632.*

Conclusion and Recommendations

> The supreme art of war is to subdue the enemy without fighting.
>
> —Sun Tzu, *The Art of War*

Russia's near-abroad strategy is to maintain a sphere of influence in former Soviet states and at the same time disrupt EU and NATO's involvement in the area. It uses an operational concept that destabilizes East-European NATO and non-NATO countries, in the latter by seizing vital terrain in a covert manner that ensures permanent gain to block NATO membership. The operational concept provides a framework that uses Russian operational art's lasting tenets, foundations, ways, and military means expanded with non-military means linked to social conditions, and the cyber domain. It entails a combination of means and domains that pose a challenge to the current Western way of war and that can be used outside the near abroad, giving the operational concept a broader application.

Non-military Means and Social Conditions

Current Russian operational art uses non-military means to mitigate adversaries' capabilities and allow Russia to achieve its objectives preferably without engaging in conventional battle. It is a whole-of-society approach that uses state owned or controlled assets, ministerial departments, non-governmental institutions, and proxy forces as means for its operations to reach the desired end state. These non-military means engage simultaneously and speedily throughout the entire depth in all physical and information domains, through application of asymmetric and indirect actions, creating chaos, seizing vital terrain, and isolating enemy leadership.

The predominant non-military means Russia relies on are media and paramilitary organizations. Russia has integrated her civil and military media to shape perception at home, in the targeted country, and within the international community in a continuous information war. It

uses information warfare techniques based on one-sidedness of information and information blockade to deceive, tempt, intimidate, and disinform the targeted audience. To establish information domination in the targeted country, Russia procures local media and social media. Blogger communities that propagate the Russian cause, and the ability to shutdown popular Internet sites that spread anti-Russian messages, aid the Russian cause.

The paramilitary consists of local, mostly ethnic Russian, organizations and volunteers from abroad. Laws in former Soviet states prohibit Russian as an official language and create discrimination towards Russian culture and heritage, leading to feelings of marginalization. Russian media targets areas that contain a significant demographic ethnic Russian-minority, emphasizing their Russian heritage based on language, history, and unique Russian culture. These narratives enhance the minorities' feelings of marginalization by their government (fear), a sense of self-worth and belonging (honor), and a perception that Mother Russia has more to offer than the native country (interest). They create involvement in social activity, community networks, and provide a forum to explore personal rights. Russia builds strong relations with local ruling elites that are willing to cooperate and form (military) organizations. In the same way, Russia creates cyber proxy forces and appeals to other organizations such as youth groups, cybercrime, and Cossacks. The proxy forces receive help from private (military) companies, bankers, Russian peacekeeping forces, and SOF conducting unconventional warfare, to organize, train, equip, and finance an effective uprising.

Russian media also address the population of the targeted country to isolate their government cognitively from their people and raise support for intervention. The media campaign emphasizes that the government is not legal, is not in control, is not serving their interest, and will lead them in a useless war they cannot win legally nor militarily. Russia uses cyber denial of service attacks to physically restrict and isolate the targeted government, local and national political and military leaders, preventing them from sending, receiving, or gaining (other)

information. Cyber proxy forces supported by cybercrime companies conduct these attacks. They also instigate attacks against financial institutions to create chaos. Finally, Russian media targets the international community on international legal matters.

Russia uses legal deniability and justification within international laws for their operations. Paramilitary forces, civil organizations, and SOF act as volunteers with no ties to Russia and cyber-crime companies and cyber proxy forces claim to work on their own. They provide Russia with legal deniability, deception, and concealment of their actions and intentions. These means allow Russia to maneuver within international law and order and prevent international pressure and intervention. The ethnic Russian minority provides Russia with a justification for its actions, to protect Russians abroad, justified by UN Article 1 on the right to self-determination. Russia uses broad interpretations of international laws to justify their actions to the UN, the West, the Russian population, and to the government and population of the targeted country. It also outmaneuvers international laws that deal with cyber-attacks, as cyber-attack means are not an "armed force" as Article 51 of the UN charter describes nor the outcome of an "armed conflict," as Russia makes sure that there are no organizational and technical links to the cyber-attacks.

With the help of the media, non-military means, social unrest, and a legal framework, the Russian operational approach generates psychological effects of reflexive control to influence the behavior of actors in such a way that they undertake actions favoring the Russian plan, ultimately leading to a sense of despair. Reflexive control uses cognitive or behavioral characteristics of an individual or group to create a cognitive model that delivers an approach how to persuade them. Russia thoroughly analyzes the enemy, the characteristics and weaknesses of his command and control system, and his willingness to fight, in order to arrange interdependent sequential reflexive control mechanisms that degrade the enemy's willingness to fight, leading to

operational shock and, ultimately, strategic paralysis. At this point, enemy leadership will be in despair and willing to sign a treaty with Russia, transforming the conflict into a frozen one.

Predict, Anticipate, and Counter

Though Russian military leadership states that its operational art uses non-military means and ways flexibly and adapts to local conditions, the *modus operandi* of the non-military means within the operational framework and its links to social conditions, for now, seem to remain constant.[160] The annexation of Crimea by Russia inspired pro-Russian actors in East Ukraine to bolster an uprising similar to that in Crimea.[161] NATO intelligence revealed Russian supply and troops support, lifting the blanket of concealment and preventing Russia the ability to deny involvement. This led to international pressure and involvement.

Currently, NATO supports non-NATO members by offering membership and Security Forces Assistance. Next, it supports East-European NATO members by stationing forces in their countries and conducting exercises, though in a very limited way. Although NATO military actions are limited, these actions could backfire on NATO as Russia will use them for their media campaigns, while also encouraging Russia to expedite its operations to stop NATO expansion. States that pursue NATO membership and contain ethnic Russian minorities still are possible targets. Furthermore, NATO countries with a large ethnic Russian minority provide Russia with opportunities to test the strength and resilience of NATO.

Instead, NATO should use its warnings and indicators system to anticipate Russian moves based on the operational framework and block reflexive control mechanisms from being achieved, effectively stopping one phase from evolving into another. Warning that Russia is covertly starting a crisis is feasible as NATO could monitor indicators such as media, cyber

---

[160] Gerasimov; Van Herpen, 247; Merle Maigre, *Crimea – The Achilles' Heel of Ukraine* (Talinn, Estonia: International Centre for Defence Studies, 2008), 1-21.

[161] Woehrel, 1.

activity, social unrest, and movements of groups of men of military age to these countries. Additionally, to counter this psychological warfare, NATO must prevent isolation of a nation's leadership. The current crisis in East Ukraine shows how NATO can counter this, by providing intelligence assets that reveal Russian involvement. Counter information warfare with media means broadcasting in Eastern Europe to mitigate the Russian information dominance is another option. However, these are all reactive measures.

Ideally, NATO should counter Russia before the conflict escalates. The Russian whole-of-society approach needs Russians at home and abroad that are willing to join the fight because they feel marginalized. A first step in easing tensions might well be that former Soviet states resolve the marginalization of ethnic Russians in their society, taking in account their needs and rights. Additionally, to shape a stable region and counter Russian influence tactics, it is beneficial for NATO to know how Russian minorities view reunification with Russia, including a way to influence their view. Further research on how to counter Russian operations as early as possible is necessary. While NATO focusses on military answers to the Russian threat, the most effective answer might well be in improving social conditions.

For the latter, NATO could refine its concept of engagement in such a way that regular units stationed in Eastern Europe understand and address the social grievances in the area as part of a whole-of-government approach. The purely military deterrence in Eastern Europe then also becomes a phase zero mission, preventing Russia from escalating. Finally, NATO could adopt and refine the recently developed USSOCOM counter-unconventional warfare method that addresses most of the non-military means it has to counter. The method does not specifically address the Russian operational framework and therefore does not describe the links between non-military means, social conditions, and cyber-attacks. Based on this monograph, NATO could refine it to a specific anti-Russian counter-unconventional warfare approach with a focus on interdependencies, to degrade the Russian reflexive control system and prevent the cumulative

effect it has. A prerequisite is the ability to operate in the cyber domain as part of the human domain, and should therefore be part of the counter unconventional warfare method.

Bibliography

Books

Berger, Peter L., and Thomas Luckmann. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge.* New York: Doubleday, 1966.

Gammer, Moshe. *The Lone Wolf and the Bear: Three Centuries of Chechen Defiance of Russian Rule*. Pittsburg, PA: University of Pittsburg Press, 2006.

Gongora, Thierry, and Harald Von Riekhoff. *Toward a Revolution in Military Affairs?: Defense and Security at the Dawn of the Twenty-First Century.* Santa Barbara, CA: Greenwood Publishing Group, 2000.

Gvosdev, Nikolas K, and Marsh, Christopher. *Russian Foreign Policy Interests, Vectors, and Sectors.* Thousand Oaks, CA: CQ Press, 2014.

Jackson, Nicole J. *Russian Foreign Policy and the CIS: Theories, Debates, and Actions.* London, UK: Routledge, 2003.

Kipp, Jacob W. "The Tsarists and Soviet Operational Art." In *The Evolution of Operational Art: From Napoleon to the Present*, edited by John Andreas Olsen and Martin van Creveld, 64-95. New York, NY: Oxford University Press, 2011.

Marsh, Christopher. "Eastern Orthodoxy and and the Fusion of National and Spiritual Security." In *The Routledge Handbook of Religion and Security.* Editors Chris Seiple, Dennis R. Hoover and Pauletta Otis, 22-32. Abingdon, UK: Routledge, 2013.

———. "Orthodox Spiritual Capital and Russian Reform." In *The Hidden Form of Capital*. Editors Peter L. Berger and Gordon Redding, 171-190. London, UK: Anthem Press, 2010.

Naveh, Simon. *In Pursuit of Military Excellence: The Evolution of Operational Theory*. Abingdon, UK: Frank Cass Publishers, 1997.

Nygren, Bertil. *The Rebuilding of Greater Russia: Putin's Foreign Policy towards the CIS Countries.* Abingdon, UK: Routledge, 2008.

Service, Robert. *A History of Modern Russia from Nicholas II to Vladimir Putin.* Cambridge, MA: Harvard University Press, 2005.

Tzu, Sun. *The Art of War*. Translated by Lionel Giles. Project Gutenberg Ebook, 2008. Kindle ed.

United Nations (UN). *Charter of the United Nations.* New York, NY: United Nations, 1945.

Van Evera, Stephen. *Guide to Methods for Students of Political Science.* Ithaca, NY: Cornell University Press, 1997.

Van Herpen, Marcel H. *Putin's War: The Rise of Russia's New Imperialism*. Lanham, MD: Rowman and Littlefield, 2014.

Von Clausewitz, Carl. *On War*. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1989.

Wilson, Andrew. *The Ukrainians, Unexpected Nation*. London, UK: Yale University Press, 2009.

Russian Federation Sources

Chekinov, Sergey. G., and Sergey. A. Bogdanov. "The Nature and Content of a New-Generation War." *Voyennaya Mysl* 10, no. 4 (2013): 13-24.

Foreign Broadcast Information Service Central Eurasia. "Military Doctrine of the Russian Federation." 2010. Accessed 10 July 2014. http://news.kremlin.ru/ref_notes/461.

Gerasimov, Valery. "The value of science in anticipation." *VPK news*. 27 February 2014. Accessed 2 July 2014. http://www.vpk-news.ru/articles/14632.

Isserson, Georgii S. "The Evolution of Operational Art." Translated by Bruce W. Menning. Fort Leavenworth, KS: SAMS Theoretical Special Edition, 2005.

Kopytko, Vasily K. "Evolution of Operational Art." *Voyennaya Mysl* 17, no. 1 (2008): 204-214.

Ministry of Defense. *The Priority Tasks of the Development of the Armed Forces of the Russian Federation*. Moscow: The Defense Ministry of the Russian Federation, 2003.

Shemayev, Volodymyr N. "Cognitive Approach to Modeling Reflexive Control in Socio-Economic Systems." *Information and Security* 22 (2007): 28-37.

Smolovyi, A.V. "Problemniye voprosy sovremennogo operativnogo iskusstva i puti ich rescheniya." *Voyennaya Mysl*, no. 12 (2012): 21-24.

US Governmental Sources

Central Intelligence Agency. "Kremlin Allies' Expanding Control of Runet Provokes Only Limited Opposition." *Media Aid* (28 February 2010): 1-17.

Department of the Army. Army Doctrine Reference Publication (ADRP) 3-0, *Unified Land Operations.* Washington, DC: Government Printing Office, 2012.

———. Army Doctrine Reference Publication (ADRP) 5-0, *The Operations Process.* Washington, DC: Government Printing Office, 2012.

———. *Counter-Unconventional Warfare.* Washington, DC: Department of the Army, 2014.

Joint Chiefs of Staff. Joint Publication (JP) 1.02, *Dictionary of Military and Associated Terms.* Washington, DC: Department of Defense, 2013.

———. Joint Publication (JP) 5-0, *Joint Operation Planning*. Washington, DC: Department of Defense, 2014.

Research

Bērziņš, Jānis. *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. Riga, National Defense Academy of Latvia, Center for Security and Strategic Research, 2014.

Blank, Stephen J. "No Need to Threaten Us, We Are Frightened of Ourselves. Russia's Blueprint For a Police State, the New Security Strategy." In *The Russian Military Today and Tomorrow - Putin, Russian Navy, Ukraine, Gazprom, Rosneft, Lavrov, Deep Operations, Campaign Design, Russian-Chinese Security Relations, Mafia and Arms Dealers*. Edited by Stephen J. Blank and Richard Weitz, 305-2057. Kindle Edition. Carlisle PA: Strategic Studies Institute, U.S. Army, 2014.

Boyd, Bradley L. "Cyber Warfare: Armageddon in a Teacup?" Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2009.

Gallup. *Contemporary Media Use in Ukraine.* Washington, DC: Broadcasting Board of Governors, 2014.

Cabayan, Hriar, David Adessnik, Chandler Armstrong, Allison Astorino-Courtois, Lt Col Alexander Barelka, Thomas Bozada, David Browne, Charles Ehlschlaeger, Dana Eyre, LTG Michael Flynn, LTC John Ferrell, LeAnne Howard, Robert Jones, David Krooks, Anne McGee, Timothy Perkins, Dan Plafcan, and Lucy Whalley. *Operational Relevance of Behavioral and Social Science to DoD Missions.* USA: Sarah Canna, NSI Team, March 2013.

Cohen, Ariel, and Robert E. Hamilton. "The Russian Military and the Georgian War: Lessons and Implications." Monograph, Strategic Studies Institute, U.S. Army, Carlisle, PA, 2011.

Davydov, Igor. "The Crimean Tatars and their Influence on the "Triangle of Conflict" — Russia-Crimea-Ukraine." Paper, Naval Postgraduade School, Monterey, CA**,** 2008.

Donovan, George T. "Russian Operational Art in the Russo-Georgian War of 2008." Strategy Research, US Army War College, Carlisle Barracks, PA, 2009.

Ginos, Nathan D. "The Securitization of Russian Strategic Communication." Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2010.

Haas, Marcel de. "Russia's Military Doctrine Development (2000-2010)." In *Russian Military Politics and Russia's 2010 Defense Doctrine.* Edited by Stephen J Blank, 1-61. Carlisle, PA: Strategic Studies Institute, U.S. Army, 2011.

Heickero, Roland. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.* Stockholm, Sweden: Swedish Defence Research Agency, 2010.

Hoffman, F. G., and T. X. Hammes. *Joint Force 2020 and Human Dynamics: Time for a New Conceptual Framework?* Washington, DC: Center for Strategic Research, National Defense University, 2013.

Information Handling Services (IHS) Jane's. *Jane's Sentinel Security Assessment - Russia And The CIS.* Englewood, CO: IHS Global Limited, 2014.

Kipp, Jacob W. "Russian Military Doctrine: Past, Present, and Future," in *Russian Military Politics and Russia's 2010 Defense Doctrine.* Edited by Stephen J. Blank, 63-151. Carlisle, PA: Strategic Studies Institute, U.S. Army, 2011.

———. "Operational Art and the Curious Narrative on the Russian Contribution: Presence and Absence Over the Last 2 Decades." In *The Russian Military Today and Tomorrow - Putin, Russian Navy, Ukraine, Gazprom, Rosneft, Lavrov, Deep Operations, Campaign Design, Russian-Chinese Security Relations, Mafia and Arms Dealers*. Editors Stephen J. Blank, and Richard Weitz, 2624-3634. Kindle Edition. Carlisle PA: Strategic Studies Institute, U.S. Army, 2014.

Maigre, Merle. *Crimea – The Achilles' Heel of Ukraine.* Talinn, Estonia: International Centre for Defence Studies, 2008.

Manwaring, Max G. *The Complexity of Modern Asymmetric Warfare*. Norman, OK: University of Oklahoma Press, 2012.

McAfee. *Virtual Criminology Report 2009*. Santa Clara, CA: McAfee, 2009.

Neukirch, Claus. *Russia and the OSCE- The Influence of Interested Third and Disinterested Fourth Parties on the Conflicts in Estonia and Moldova*. Flensburg, Germany: Centre for OSCE Research, 2001.

Ohana, Yael. *Supporting Cultural Actors of Change in Belarus, Moldova and Ukraine: A Regional Review.* Washington, DC: The German Marshall Fund of the United States, 2008.

Shnirelman, Victor. "New Racism, Clash of Civilisations and Russia." In *Russian Nationalism and the National Reassertion of Russia.* Editor Marlene Laruelle, pg#s. Abingdon, UK: Routledge, 2009.

Socor, Vladimir. "Nord Stream Project: Bilateral Russo-German, Not European." *Eusasia Daily Monitor* 4, no. 179 (2007). Accessed 1 September 2009. http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=33033&no_cache=1#.VAUMVsVdW_s.

Statie, Mihai-Cristian. "Transnistria: The 'Hot' Nature of a 'Frozen' Conflict." Monograph, School of Advanced Military Studies, Fort Leavenworth, KS, 2013.

Thomas, Timothy L. *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness.* Fort Leavenworth, KS: Foreign Military Studies Office, 2011.

US Cyber Consequences Unit (US-CCU). *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008.* Washington, DC: US-CCU, 2009.

Woehrel, Steven. *Ukraine: Current Issues and U.S. Policy*. Washington, DC: Congressional Research Service, 2014.

Zaborsky, Victor. "Crimea and the Black Sea Fleet in Russian-Ukrainian Relations". Discussion Paper 95-11. Harvard University, Cambridge, MA, 1995.

Journals and Articles

Babich, Dmitry. "Media wars around Crimea: Russia not impressed by liars' empty threats." *The Voice of Russia.* 20 March 2014. Accessed 4 October 2014. http://voiceofrussia.com/2014_03_20/Russia-not-impressed-by-liars-empty-threats-1813/.

Bolen, John. "Operational Art goes Digital: Information Warfare and the Future of Russian Operational Theory." *New Horizons* 7, no. 1 (April 2013): 26-38.

Bugajski, Janusz. "Georgia: Epicenter of Strategic Confrontation." *Centre for Strategic and International Studies (CSIS).* August 12, 2008.

———. "The Shadow War." *Central Europe Digist* (9 May 2014): 2-3.

Blank, Stephen. "Russian Threats to Moldova and the Balkans." *Central Europe Digist* (9 May 2014): 10-11.

Brandom, Russel. "Cyberattacks Spiked as Russia Annexed Crimea." *The Verge.* 29 May 2014. Accessed 4 October 2014. http://www.theverge.com/2014/5/29/5759138/malware-activity-spiked-as-russia-annexed-crimea.

Coalson, Robert. "Pro-Russian Separatism Rises In Crimea As Ukraine's Crisis Unfolds." *Radio Free Europe.* 18 February 2014. Accessed 24 November 2014. http://www.rferl.org/content/ukraine-crimea-rising-separatism/25268303.html.

Crandall, Matthew. "Hierarchy in Moldova-Russia Relations: the Transnistrian Effect." *Studies of Transition States and Societies* 4, no.1 (2014): 3-15.

Croft, Adrian, and Peter Apps. "NATO websites hit in cyber attack linked to Crimea tension." *Reuters.* 16 March 2014. Accessed 4 October 2014. http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316.

Daily News Bulletin. "Cossack Volunteers to Help South Ossetia." *Daily News Bulletin*. English edition. 8 August 2008.

Diuk, Nadia. "EuroEuromaidan: Ukraine's Self-Organizing Revolution." *World Affairs.* April 2014. Accessed 27 January 2015. http://www.worldaffairsjournal.org/article/euroEuromaidan-ukraine%E2%80%99s-self-organizing-revolution.

Gordon, Michael R. “Russia Displays a New Military Prowess in Ukraine’s East.” *The New York Times*, 21 April 2014. Accessed 2 July 2014. http://www.nytimes.com/2014/04/22/world/europe/new-prowess-for-russians.html?_r=0.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Security* 4. no. 2 (2011): 49-60.

Hollis, David. “Cyberwar Case Study: Georgia 2008.” *Small Wars Foundation.* 6 January 2011. Accessed 7 September 2014, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

Kaufman, Andrew. “How Dostoevsky and Tolstoy Explain Putin’s Politics.” *Andrew D. Kaufman.* 7 April 2014. Accessed 24 November 2014. http://andrewdkaufman.com/2014/04/dostoevsky-tolstoy-explain-putins-politics/.

Kirsch, Cassandra M. “Science Fiction No More: Cyber Warfare and the United States.” *Denver Journal of International Law and Policy* 40 (2012): 620-647

Laruelle, Marlene. “Negotiating History, Memory Wars in the Near Abroad and Pro–Kremlin Youth Movements.” *Demokratizatsiya [Democratization]* 8, no.4 (2000): 233-252.

Mattsson, Peter A. and Niklas Eklund, “Russian Operational Art in the Fifth Period: Nordic and Arctic Applications,” Revista de Ciências Militares, Vol. 1, No 1 (May 2013): 29-47.

Nederlands Omroepstichting (NOS). “Referendum Autonomie Krim Eerder [Referendum Crimea Earlier].” *Nederlandse Omroep Stichting [Netherlands Broadcasting Foundation]*. 1 March 2014. Accessed 4 October 2014. http://nos.nl/artikel/617563-referendum-autonomie-krim-eerder.html.

———. “Wie is de Baas op de Krim [Who is the Boss of the Crimea].” *NOS*. 11 March 2014. Accessed 4 October 2014. http://nos.nl/artikel/622011-wie-is-de-baas-op-de-krim.html.

———. “Russen Vallen Basis Krim Aan [Russians Attack Crimea Basis].” *NOS*. 7 March 2014. Accessed 4 October 2014. http://nos.nl/artikel/620412-russen-vallen-basis-krim-aan.html.

———. “Pro-Rusland-Campagne op Dreef [Pro-Russia-Campaign on a Roll].” *NOS*. 13 March 2014. Accessed 4 October 2014. http://nos.nl/artikel/622506-proruslandcampagne-op-dreef.html.

———. “Militaire Spanning Krim Stijgt [Military Tension Crimea Rises].” *NOS*. 28 February 2014. Accessed 4 October 2014. http://nos.nl/artikel/617230-militaire-spanning-krim-stijgt.html.

———. “Kiev: Invasie door Russisch Leger [Kiev: Invasion by Russian Army].” *NOS*. 28 February 2014. Accessed 4 October 2014. http://nos.nl/artikel/617425-kiev-invasie-door-russische-leger.html.

———. “Internationale Missie Oekarine [International Mission Ukraine.” *NOS*. 1 March 2014. Accessed 4 October 2014. http://nos.nl/artikel/617484-internationale-missie-oekraine.html.

Organization for Security and Co-operation in Europe (OSCE). “Transdniestrian Conflict, Origins and Main Issues.” *OSCE*. 10 June 1994. Accessed 22 August 2014. http://www.osce.org/moldova/42308?download=true.

Ray, Julie and Neli Esipova. “Russians Rely on State Media for News of Ukraine, Crimea. Few trust Western media or independent Russian media.” *Gallup World*. July 2014. Accessed 4 October 2014. http://www.gallup.com/poll/174086/russians-rely-state-media-news-ukraine-crimea.aspx.

Reid, Clifford. “Reflexive Control in Soviet Military Planning,” in *Soviet Strategic Deception*, edited by Brian Dailey and Patrick Parker. Stanford, CA: The Hoover Institution Press, 1987.

Remus, Titiriga. “Cyber-attacks and International law of armed conflicts; a jus ad bellum perspective.” *Journal of International Commercial Law and Technology* 8, no.3 (2013): 179-189.

Rogoza Jadwiga and Agata Dubas. “Russian Propaganda War: Media as a Long – and Short-range Weapon.” *Centre of Eastern Studies Commentary* 9 (11 September 2008): 1-5.

Shackelford, Scott J. “Estonia Three Years Later: A Progress Report on Combating Cyber Attacks.” *Journal of Internet Law* (February 2010): 22-29.

Yuhas, Alan. “Russian Propaganda over Crimea and the Ukraine: How Does it Work?” *The Guardian.* 17 March 2014. Accessed 4 October 2014. http://www.theguardian.com/world/2014/mar/17/crimea-crisis-russia-propaganda-media.

Weitz, Richard. “Russia Refines Cyber Warfare Strategies.” *World Politics Review*.25 August 2009. Accessed 7 September 2014. http://www.worldpoliticsreview.com/articles/4218/global-insights-russia-refines-cyber-warfare-strategies.

Williams, Michael John. “Tomorrow’s War Today.” *Central Europe Digist* (9 May 2014): 8-9.

Databases

Advameg, Inc. “Georgia.” Countries and their Cultures Database. Accessed 7 September 2014. http://www.everyculture.com/Ge-It/Georgia.html#ixzz3CHXlfxMG.