CYBER BEAR: RUSSIAN CYBER THREAT TO ITS NEIGHBORS AND AMERICA

by

Khatuna Mshvidobadze

A Capstone Project Submitted to the Faculty of

Utica College

December 2014

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Cybersecurity

Abstract

This paper examines how contemporary Russia's political, economic and social characteristics have promoted multiple cyber threats to neighboring countries and to the U.S. The utility of this study is that it may help to inform the American foreign policy public about this important matter. The paper illustrates the Russian approach to information warfare (IW) and its subset, cyber warfare. In particular, the study demonstrates how Russia's IW doctrine is tied to its geopolitical ambitions and how the relationship between the government and cyber criminals is formed in this regard.

Four major themes emerge from this study. The first is that the dominant characteristic of the Russian polity is corruption, presided over by President Vladimir Putin, and dominated by the *siloviki,* people from the security services and their entourages. The second theme is that, because the corruption is systemic, not sporadic, there is a unique Russian nexus of government, business and crime, which creates the opportunity for collusion on everything. The third theme is that this collusion fits into a long-standing and well thought out IW doctrine, which includes cyber. Putting the first three themes together, cyber criminals have become an asset in furthering Russia's interests abroad, as defined by Putin and the *siloviki.*

This study examines the root causes of Russian cyber threats, concluding that systemic corruption combines with Russia's current geopolitical aims to produce threats to Russia's neighbors and to the U.S. These are poorly understood by Americans, possibly because of different approaches to the subject.

Keywords: Cybersecurity, Christopher Riddell, Khatuna Mshvidobadze, Russia, cyber, corruption, Putin.

Acknowledgments

Working on my cyber security program and Capstone project was a very interesting and challenging process. I would like to take this opportunity to acknowledge not only those people who led me through the Capstone project, but also those who helped and supported me during my entire dual Master of Science program in cyber forensics and intelligence.

First, I would like to express my gratitude and respect for the Chair of the Cybersecurity program at Utica College, Professor Joseph V. Giordano, for all of his support and assistance throughout two and a half years. I also would like to thank Paul De Souza, President of the Cyber Security Forum Initiative, for his trust and recommendation for me to be enrolled in the program.

I also would like to thank my professor and friend Jeffrey S. Bardin for his advice and assistance as a second reader of my Capstone project. Moreover, his courses on cyber intelligence and counterintelligence were the best during the entire program.

My great appreciation also goes to Professors Christopher Riddell and Jesus Lopez for guiding me during the Capstone project writing process.

My greatest thanks must go to my husband, David J. Smith, for being a friend, advisor, supporter and encourager during the entire MS program. If not for his love, patience and belief in me, I would not have been able to accomplish so many things in my life. I would also like to thank my daughter Salome for being a friend and supporter. Finally, I am eternally grateful to all of those people who believed in me and encouraged me during every phase of my life.

Table of Contents

Cyber Bear: Russian Cyber Threat to its Neighbors and America

In today's world of perpetual news, events like the 2007 and 2008 Russian cyber-attacks on the countries of Estonia and Georgia, cyber espionage against Ukraine and Lithuania with malware called Uroburos and the exploits of the Energetic Bear advanced persistent threat (APT) are noticed by only a few and soon forgotten by most. Indications that Uroburos is related to Agent.BTZ, malware, which was used in espionage against the United States of America (U.S.), receive even less attention. Consequently, such challenges are dealt with inadequately, most often treated as singular events, rather than as elements of a syndrome. Nonetheless, albeit slowly and cautiously, there is a growing sense in the U.S. and other western countries, that is, generally the democracies of western Europe and the English-speaking world, that Russia may be the source of multiple cyber threats. Contrasting his views on the Chinese cyber threat, U.S. Director of National Intelligence James Clapper told an audience on October 16, 2014, "I worry a lot more about the Russians" (Gorman, 2014, para. 2). Russian cyber threats may present a challenge not only to Russia's neighbors, that is, the countries of the former Soviet Union and some of those of the Warsaw Pact, but also to the U.S.

Largely, due to the major attention devoted to the Chinese cyber threat, the Russian cyber threat is often overlooked and should be better understood. Former American cyber security coordinator Richard A. Clarke in his book *Cyber War,* wrote, "U.S. intelligence officials do not, however, rate China as the biggest threat to the U.S. in cyber space. 'The Russians are definitely better, almost as good as we are,' said one American official" (Clarke, 2010, p. 145). Jeffrey Carr, a cyber expert who studied the 2008 Russian cyber-attack on Georgia wrote, "Unlike China, Russian cyber operations are rarely discovered, which is the true measure of a successful op" (Carr, 2009, para. 3). As Clapper, Clarke and Carr suggested, Russian cyber operations may

sometimes go undetected because of the perpetrators' skill. However, outside observers may also have difficulty understanding what they see amid the Russian approach and organization, which is different from that of the U.S. and other western countries.

The purpose of this research was to examine how certain systemic characteristics of contemporary Russia, including its political economic and social systems, have promoted multiple cyber threats to neighboring countries and to the U.S. The utility of this study is that it may help to inform the American foreign policy public about this important matter. The research answered the following questions: What is the Russian approach to information warfare (IW) and its subset, cyber warfare? How is Russia's doctrine on IW tied to its geopolitical ambitions? What is the relationship between the Russian government and Russian cyber criminals in this regard? Does Russian cyber espionage pose a threat to neighboring countries such as Ukraine and Georgia and to the United States?

Part of the problem addressed in this study is that not only is the Russian approach to IW different from U.S. approaches it is much more developed than American thinking. Consequently, if Russia does pose a cyber threat to the U.S., it is a well-developed threat. In contrast to the U.S. government, which is still debating just about every facet of cyber policy, the Russian government has a well-developed cyber warfare doctrine—what it is, how Russia will meet it and how cyber warfare will be conducted (Smith, 2014a). This doctrinal or strategic thinking is rooted in the teachings of Marshal of the Soviet Union Nikolai Ogarkov in the 1970s and 1980s, in what he referred to as the military technical revolution (MTR). A brief restatement of his thesis is that computers, along with accuracy and miniaturization, were about to transform the modern battlefield, that America was far ahead in these fields and therefore, the Soviet armed forces needed to embrace rapid technological modernization (Metz & Kievet, 1995). By the mid-

1990s, the Russian Federation, which in many ways is a continuation of the Soviet Union without the ideological superstructure of communism, had a well-developed cyber warfare doctrine.

To use a political science term, Russia securitized IW, which would later include cyber matters, in the early 1990s. Securitization, a concept introduced by Arnold Wolfers (1952) and developed by Barry Buzan (1997), is the process of a country addressing a threat outside normal means, that is, not as a technical or legal matter, but as an existential threat warranting extraordinary attention. The U.S. did this with the Soviet nuclear threat and with the post September 11, 2001, terrorist threat. However, it has not done this with the cyber threat, despite some advocating such attention (Hare, 2010). To the contrary, as stated by James A. Lewis, Center for Strategic and International Studies Senior Fellow, "There's a kind of willful desire not to admit how bad things are, both in government and certainly in the private sector" (Barrett, 2012, para. 7). This is an important dimension of the problem addressed by this study because the Russian government may be placing extraordinary emphasis on a threat to the U.S. that the American government perceives to be an ordinary challenge among many others.

Although the roots of all this extend through the years when Russian President Boris Yeltsin was in power (1991-1999) back to Soviet times, Moscow's attention to IW and, as the Russian government views it, its subset cyber warfare, intensified during the Vladimir Putin years (1999-present, as prime minister, president, prime minister and, again, president). Under Putin, Russia's cyber capabilities and organization combined with systemic corruption and post imperial ambitions to develop multiple Russian cyber threats, not only to Russia's neighbors, but also to the U.S.—Russian military actions against U.S. allies, Russian espionage against

neighbors, U.S. allies and the U.S., and officially overlooked Russian-origin crime directed against victims around the world.

The Russian government's new security strategy, published in 2009, combines themes and tones of insecurity, resentment and aggression that demonstrate that Russia is a revisionist power with global geopolitical ambitions. For example, one major focus of the strategy is gaining and maintaining access to areas outside Russian territory. “Attention of long-term international policy perspectives will be concentrated on accessing energy resources in the Middle East, on the Barents Shelf, the Caspian Sea Basin and in Central Asia” (Russian Federation, 2009, para. 11). Another portion of the Russian government’s security strategy that captured considerable western attention is devoted to the Russian government’s objectives in the Arctic region (Russian Federation, 2009).

Like the concept of securitization, Russia as a revisionist power bears directly on the problem addressed by this study. The concept of a revisionist power was introduced to the field of international relations by A.F.K. Organski in his 1958 book *World Politics*, revised a decade later (1968). Revisionist states are unhappy with the global status quo and, as they become more powerful, become more likely to challenge the dominant, or hegemonic, power, which today is the U.S. This may begin in the geographical region of what Organski calls a middle power, however, as the middle power becomes a great power, it becomes more likely to challenge the dominant power (Organski, 1968). A half century ago, Organski was concerned with the possibility of kinetic war, however, the nature of international conflict is changing, and IW is both a cause and an effect of that change.

When Organski wrote, to challenge the hegemon, a rising middle power would have had to accumulate sufficient strength among the traditional measures of power—military, financial,

population and territory (Organski, 1968). Today, depending on their objectives, weaker nation-states and even sub-national and trans-national groups, may be able to challenge the U.S. Chinese People's Liberation Army Colonels Qiao Liang and Wang Xiangsui describe this as a transition to unrestricted warfare (2002). Unrestricted warfare does not mean extreme or intemperate warfare; rather, it means warfare that is not restricted by the traditional bounds of the physical battlefield, specialized weapons and distinct warriors. Technology and a different way of thinking mean that the battlefield could be everywhere or nowhere, weapons could be ordinary items that have dual uses and anyone could become a combatant. "Who is the most likely to become the leading protagonist on the terra incognita of the next war" ask Qiao and Wang? "The first challenger to have appeared, and the most famous, is the computer 'hacker'" (Qiao and Wang, 2002, p. 33). They continue:

> Any war that breaks out tomorrow or further down the road will be characterized by warfare in the broad sense—a cocktail mixture of warfare prosecuted through the force of arms and warfare that is prosecuted by means other than the force of arms. (Qiao and Wang, 2002, p. 43)

We may now be seeing Qiao and Wang's concept of unrestricted warfare applied to Russia's transition from a middle power to a revisionist great power, in Organski's terms. The first steps would be taken in the rising middle power's geographical region. Traditionally, there have been three, not mutually exclusive, methods used by the Russian government against former Soviet states. First are measures such as energy manipulation, economic embargoes, blackmail, extortion, political subversion, etc. For example, Russia failed to cow the government of the country of Georgia with such methods, which was one reason for its resorting to the second method, which is direct military invasion. The third method, as defined by Anatoly Chubais,

former Russian chief of privatization policy and later chief of the government energy holding company, UES, is liberal imperialism. This is intended to keep countries encompassing the former Soviet Union economically dependent on Russia (Torbakov, 2003).

Cyber warfare may be emerging as another, cost effective, way to attempt to subdue the countries of the former Soviet Union and the Warsaw Pact. It can be used as a stand-alone capability, that is, as a fourth method, or as a complement to any or all of the other three. Attacks aimed at cowing neighboring governments into submission that have incorporated a cyber element have been seen in Estonia in 2007, Georgia in 2008, and, to a different extent, during the 2013-2014 crisis over Ukraine's association agreement with the European Union (E.U.) (Smith, 2014b).

The cyber-attack on Estonia began on April 26, 2007, after its government decided to relocate a Soviet war memorial away from the Tallinn city center. The initial targets were Estonian government websites, but later focus shifted to services such as banks, telephone exchanges, and the emergency services telephone numbers, akin to 911 in the U.S. The most intense attack against Estonian targets occurred on May 9, 2007. May 9, referred to as Victory Day, is the day Russia annually celebrates the Soviet Union's victory over Nazi Germany (Kelly & Almann, 2008). This was an example of a combination of political subversion and cyber-attacks.

In 2008, the country of Georgia was attacked by Russia in the first ever combined kinetic and cyber war. After a year of study, the U.S. Cyber Consequences Unit (US-CCU, 2009), an independent research institute, concluded that the cyber-attacks were an integral part of Russia's armed attack on Georgia. The cyber war coordinators were fully aware of the impending attack upon Georgia and its timing. Such an attack required advance mapping, testing, registering new

domains and creating dedicated websites. Moreover, the US-CCU report indicated that most of the botnets used against Georgia had already been used for criminal activities (US-CCU, 2009). A botnet is a collection of computers surreptitiously interconnected to combine small amounts of their computing power under the direction of a single controller, usually without the knowledge of the computer owners. Botnets are used for spamming and launching distributed denial of service (DDoS) attacks, and are often rented out as a criminal enterprise. DDoS attacks are waves of distinct cyber attacks against a particular website, and the routers and switches that support it, designed to overwhelm the target's capacity to process all of the incoming data, thus denying the website's intended function to legitimate users. In this case, there were strong implications that the Russian government acted in concert with Russian organized crime. Amateur hackers were also recruited through social networks to augment the attacks (US-CCU, 2009).

Espionage is also part of the threat faced by Russia's neighbors, however, there are strong indications of Russian involvement in cyber espionage against the U.S. Although the use of Uroburos—alternatively known as Snake or Turla—espionage malware against Ukraine and, to a lesser extent, Lithuania predated the 2013-2014 Russia-Ukraine conflict, its existence was revealed during that conflict. Moreover, most analysts—Kaspersky lab, Symantec, G-Data and BAE Systems (Apps and Finkle, 2014; How Turla, 2014; Snake, 2014; Uroburos, 2014)—who have examined this malware have concluded that it is related to Agent.BTZ, another malware worm, which led to Buckshot Yankee, the largest cyber cleanup operation in American history (Andress & Winterfeld, 2011).

There have been recent revelations that Gyges, a government-grade penetration and obfuscation malware program, possibly of Russian origin, may have been embedded within

ransomware, such as Cryptolocker. Ransomware encrypts files in an infected computer and then demands payment to decrypt them. These revelations offer another indication of the collusion between the Russian state and cyber criminals (Osborne, 2014). This is unsurprising since the Russian government sub-contracted the attacks on Estonia and Georgia to cyber-criminal syndicates like Russian Business Network (RBN) (Markoff, 2008).

Most recently, a well-resourced, possibly government-sponsored, Russian APT known as Energetic Bear or Dragonfly has been infecting energy-related industrial control systems (ICSs). Energetic Bear appears to be moving beyond computer network exploitation, although still short of a computer network attack. There is some evidence that it has been installing back doors into the systems that control some of U.S. and other western countries' critical infrastructure (Symantec, 2014).

In sum, the problem addressed by this study is that the Russian cyber threat is often overlooked and should be better understood. Part of the reason that Americans and other western observers have difficulty understanding the Russian cyber threat is that the Russians are good at what they do. However, there is another dimension, which is that the Russian approach to IW and cyber conflict is very different from that with which most westerners are familiar. The challenge is exacerbated because Russia appears to be a revisionist power, unhappy with the current world order, aggressive toward its neighbors, possibly willing to challenge the dominant position of the U.S. and seeing IW in extraordinary terms. Nonetheless, U.S. officials have become increasingly aware of the Russian cyber threat. This study aims at increasing that awareness.

Literature Review

Developing a full picture of how corruption and geopolitics in Russia combine to nurture multiple cyber threats to Russia's neighbors and to the United States requires a multi-disciplinary

approach. Consequently, understanding the interplay of geopolitics, corruption and cyber requires an examination of a multifaceted collection of literature. There are two reasons for this. First, taking into account the small amount of traditional academic literature on Russian cyber, one must resort to other sources. Second, rapid developments in the cyber field magnify the importance of journalistic accounts and the work of Internet security organizations, whether they are not-for-profit or commercial companies. Consequently, this literature review will address some traditional literature, but also monographs, articles, blogs, and studies on specific cyber cases, laws and strategic documents to present a full and accurate representation of Russian cyber threats.

Systemic Corruption in Russia

Elaine Byrne is a widely published expert on corruption, currently serving as an adviser to the European Commission. Her definition of petty corruption is the kind of corruption with which most westerners are familiar: "Small scale, bureaucratic or petty corruption is the everyday corruption that takes place at the implementation end of politics, where the public officials meet the public" (Byrne, 2009, para. 9). This sort of corruption is often sporadic corruption, which is "The opposite of systemic corruption. Sporadic corruption occurs irregularly and therefore it does not threaten the mechanisms of control nor the economy as such" (Byrne, 2009, para. 6). Systemic corruption is altogether different:

> As opposed to exploiting occasional opportunities, *endemic* or *systemic* corruption is when corruption is an integrated and essential aspect of the economic, social and political system, when it is embedded in a wider situation that helps sustain it. Systemic corruption is not a special category of corrupt practice, but rather a situation in which the major institutions and processes of the state are routinely dominated and used by corrupt

individuals and groups, and in which most people have no alternatives to dealing with corrupt officials. (Byrne, 2009, para. 5)

The two most prominent major works on corruption in contemporary Russia are *The Corporation* by Yuri Felshtinsky and Vladimir Pribylovsky and *Darkness at Dawn* by David Satter. Felshtinsky is a historian who joined with Alexander Litvinenko, allegedly killed by the Federal Security Service (FSB) in London, to expose a series of apartment bombings allegedly carried out by the FSB (Felshtinsky & Litvinenko, 2007). Satter was Moscow Bureau Chief for the *Financial Times.*

Although most of his book is anecdotal, Satter offered some incisive analysis in his Introduction. After the overthrow of the communist regime, he wrote, "Russia came to be dominated by poverty, intimidation and crime" (Satter, 2003, p. 1). The reason, he explained, is that in the rush to build a capitalist economy, rule of law was forgotten. Consequently, Satter said, Russia developed into a kleptocracy characterized by bribery, institutionalized violence, pillage and mass moral indifference (2003, p. 2). Satter described the result:

> Officials and businessmen took no responsibility for the consequences of their actions, even if those consequences included hunger and death. Government officials helped to organize pyramid schemes that victimized people who were already destitute, police officials took bribes from leaders of organized crime to ignore extortion, and factory directors stole funds marked for the salaries of workers who had already gone months without pay. (Satter, 2003, p. 2)

Felshtinsky and Pribylovsky harken back to Aristotle for a definition of contemporary Russia: oligarchy. Oligarchy, the authors recall, differs from democracy because "Rulers pursue their own interests rather than the general welfare" (Felshtinsky & Pribylovsky, 2008, pp. 180-

181). They continue, “The oligarchs are the nomenklatura elite, the president at the top” (Felshtinsky & Pribylovsky, 2003, p. 182), followed by senior government officials—federal, regional, judicial and military—and what they call business tycoons (Felshtinsky & Pribylovsky, 2003).

Felshtinsky and Pribylovsky further break down the oligarchy that surrounds President Vladimir Putin into four clans: “Old Kremlin…old Petersburg…new Petersburg…mayor’s office” (2003, p. 185). For the purpose of this research, the most important of these clans is the new Petersburg group, more commonly known as the *siloviki,* literally meaning persons of power, referring to those who came out of the security services, and their entourage. When Putin came to power, the *siloviki* deliberately set out to infiltrate every government and business organization. They are particularly influential in the arms and energy industries. Although they are certainly not against private property and profit, the *siloviki,* write Felshtinsky and Pribylovsky, believe in strong government regulation of the economy to bolster Russia’s interests and maintain law and order (Felshtinky & Pribylovsky, 2003). Reading Satter and Felshtinsky and Pribylovsky together, one forms an image of Russia ruled by an oligarchy of intertwined government officials and businessmen, run as a kleptocracy in which systemic corruption has replaced rule of law. “Laws exist,” write Felshtinsky and Pribylovsky, “but they are written by the government, for the government” (Felshtinsky and Pribylovsky, 2003, p. 181).

In this context, David J. Smith adds another important dimension. Russia, he explained, exhibits many of the characteristics of an extractive economy, similar to a third world country. However, unlike a third world country, it is also heir to the very good Soviet educational system. Wealth is concentrated in the hands of the oligarchs while many people with good educations in math and the hard sciences remain unemployed (Smith, 2014a, para. 10). It is unsurprising, then,

that cyber-crime thrives in contemporary Russia. Moreover, given the potential that cyber offers for profits, social control at home and coercion beyond Russia's borders, it is also unsurprising that various cyber endeavors have attracted the attention of the people at the center of what Smith calls the "Nexus of government, business and crime" (Smith, 2012, p. 7).

Cyber Crime in Russia

At this point, it is useful to examine an example of another genre of literature; the specialized report written by a security company. Max Goncharov of Trend Micro authored one of the most useful pieces of this type. In *Russian Underground 101,* Goncharov (2012) wrote that the Russian shadow economy "Has become a kleptocracy wherein crony capitalism has obtained a new lease on life in cyberspace" (Goncharov, 2012, p. 25). Based on his reading of hacker-authored articles and browsing of cybercrime forums like antichat.ru, xeka.ru and cardingcc.com, Goncharov compiled a catalog of cyber-criminal software and services for sale or rent. For example, in 2012 prices, one could contract a simple DDoS attack for $30 to $70 a day, $150 a week or $1,200 a month. One advertising post boasts, "Fabulous performance;" another offers "Continuous technical support" (Goncharov, 2012, p. 9). If one prefers to run one's own DDoS attack, one could buy a botnet for $700 (Goncharov, 2012).

There are two important points to be drawn from Goncharov's work. First, cyber-crime thrives in Russia. Second, in a country obsessed with monitoring the Internet with systems like SORM-3 (SORM-3, n.d.), criminal sites such as the aforementioned function with impunity. Such websites also persist despite the Russian government's efforts to shut down websites that it determines are unacceptable. For example, a 2012 law created a registry for sites that contain objectionable material. Government supporters say the law is only to protect children. Critics maintain that it is used to shut down sites considered to be oppositional (Andrews, 2012). The

persistence of easy to find online crime is an indicator of collusion between the state and cyber criminals.

Russian Information Warfare and Cyber Warfare Doctrine and Organization

Although cyber-crime is a post-Soviet phenomenon, Russian thinking on cyber warfare, which they see as part of IW, has Soviet roots. The development of Russian IW is described in an excellent monograph by Heickerö (2010). The Russian view of IW, Heickerö explained, can be traced back to the 1980s, particularly to Ogarkov's writings on the MTR.

Heickerö outlined how Soviet and Russian theorists subsequent to Ogarkov further developed Russian thinking on IW, which includes cyber warfare. These analysts carefully followed American literature on the revolution in military affairs, frequently referred to as the RMA, which was, in essence, an Americanized view of the MTR. They also read American literature on net-centric warfare and watched as the U.S. developed in practice the warfare that Ogarkov had presaged in theory. "They declared the Gulf War of 1990-1991 as the first technical operation" (Heickerö, 2010, p. 15).

According to Heickerö, some events inside Russia also influenced their thinking about IW. First, the Yeltsin years brought very lean budgets. Consequently, IW theorists spent time developing theory rather than building machines, writing software and running operations. Second, Russian analysts believed that Chechen rebels had gotten the upper hand in IW during the First (1994-1996) and Second (1999-2000) Chechen Wars. "Both wars in Chechnya," wrote Heickerö, "showed that in some areas, even a small and relatively impoverished adversary could achieve information dominance over a stronger opponent by using the mass media component efficiently" (Heickerö, 2010, pp. 15-16).

The result was a well-developed IW theory by the mid-1990s. Heickerö quoted a 1996 speech by then Chief of the Russian General Staff General Viktor Samsonov that is worth repeating here:

> The high effectiveness of information warfare systems in combination with highly accurate weapons and non-military means of influence makes it possible to disorganize the system of state administration, hit strategically important installations and groupings of forces, and affect the mentality and moral spirit of the population. In other words, the effect of using these means is comparable with the damage resulting from the effect of weapons of mass destruction. (Heickerö, 2010, p. 16)

Also valuable are the many works of Colonel (ret) Timothy Thomas of the U.S. Army Foreign Military Studies Office. For example, further illustrating how well developed Russian IW doctrine was in the 1990s, Thomas cited retired Colonel Vitaly Tsymbal of the Russian military. In 1995, speaking at a conference in the U.S., Tsymbal said:

> From a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not . . . considering the possible catastrophic consequences of the use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces. . .Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself. (Thomas, 1996-1997, para. 4)

Thomas places Russian thinking on cyber warfare into the broader context of operational IW and the even broader context of strategic IW. Quoting an unnamed Russian military officer,

Thomas described operational IW as actions of the "Forces and assets of intelligence and early warning, command and control, communications, deception and electronic warfare whose purpose is to guarantee the achievement of the goals of the [combat] operation" (Thomas, 1996, p. 27). On the other hand, strategic or technical/psychological IW is to exert "information/psychological and information/technical influence on a nation's decision-making system, on the nation's populous [sic]" (Thomas, 1996, pp. 26-27). Cyber warfare is just one of the many tools of IW, which takes place 24 hours a day, 7 days a week, 52 weeks a year, in wartime and in peacetime. A cyber-attack against Russia would not be considered prelude to war, but war itself, and Russia reserves the right to respond with whatever means it deems appropriate, including nuclear weapons (Thomas, 1996-1997).

In wartime, wrote Heickerö, IW is more overt, including "Distortion, deception and manipulation of information, including psychological operations…Information blockade, interpreted as using electronic saturation techniques, DDoS and spamming" (Heickerö, 2010, pp. 18-20). On the official level, the current Russian Military Doctrine, published in 2010, called for the "Prior implementation of measures of informational warfare in order to achieve political objectives without the utilization of military forces" (Russian Federation, 2010, para. 13). Note that this passage is similar to the one used by Samsonov 14 years earlier. In Russia, IW is perceived as an integrated whole of systems working together: intelligence, counterintelligence, *maskirovka*, (making things appear what they are not) disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure and destruction of enemy computer networks and software applications (Thomas, 1996-1997).

Apart from doctrinal matters, declining resources have also become a factor in the Russian military's interest in cyber. An unnamed source in the Russian military told the Russian

newspaper *Kommersant,* "With the current size of the armed forces we cannot do without the use of high-tech. This will increase the effectiveness of the troops as well as implement tasks that previously required considerable resources" (Chernenko & Safronov, 2012, para. 5). The same source also noted that the Russian Defense Ministry began actively to pursue the matter in January 2012, after Chief of General Staff General Nikolai Makarov announced the necessity of readiness for cyber war. Since then, the source continued, the General Staff's Scientific and Technical Council meets regularly with General Staff specialized units—Radio-Electronic Warfare Forces and the 8th Directorate, responsible for encryption (Chernenko & Safronov, 2012).

This revelation is all the more interesting in light of research presented at the 2011 NATO CyCon in Tallinn by Keir Giles of the Oxford Conflict Studies Research Centre. At the time, Giles presented indications that a Russian military cyber capability may have been growing in the Radio Electronic Troops (Giles, 2011). In particular, the author cited the Russian military expert, Head of the Center for Military Forecasting, Anatoly Tsyganok. According to Tsyganok:

> The personnel of the Information Troops should be composed of diplomats, experts, journalists, writers, publicists, translators, operators, communications personnel, web designers, hackers, and others... To construct information countermeasures, it is necessary to develop a centre for the determination of critically important information entities of the enemy, including how to eliminate them physically, and how to conduct electronic warfare, psychological warfare, systemic counterpropaganda, and net operations to include hacker training. (Giles, 2011, p. 52)

In the same paper, Giles also presented indications that the Russian military's interest in IW was creating friction with the FSB. The Russian Ministry of Defense frequently mentioned

the phrase “infrastructure protection,” sometimes neglecting to place the adjective military before it. This intra-governmental squabble may account for the apparent lack of follow-up to the March 21, 2012, statement of Deputy Prime Minister Dmitry Rogozin, who has responsibility for Russia's military-industrial complex: "We are currently discussing the question of setting up a cyber-security command…This is in connection with guaranteeing information for the armed forces, and also the state infrastructure as a whole” (RIA Novosti, 2012, para. 2). Nonetheless, in September 2012, the Security Council of the Russian Federation released a document that assigns critical infrastructure protection to the FSB (Russian Information Security, 2012).

Despite this apparent FSB victory over the Ministry of Defense (MoD), the latter’s efforts persist. For example, on October 7, 2012, the Russian MoD announced a tender for research in the field of information security. The competition was open to postgraduate students, research, innovation and manufacturing teams, as well as other citizens of the Russian Federation “With the potential and internal motivation to solve large-scale scientific and engineering problems for the benefit of the Russian armed forces.” Among the subjects of interest mentioned in the announcement are “methods and means of bypassing anti-virus software and firewalls and protection of networks and operating systems” (Ministry of Defense, 2012, para. 10). Valery Yashchenko, Deputy Director of the Moscow State University Institute of Information Security, commented to *Kommersant* newspaper, “This would be elements of cyber weaponry…they can be used for both defensive and offensive purposes” (Chernenko & Safronov, 2012, para. 3).

As the intra-governmental tussle over infrastructure protection illustrates, the FSB is the most powerful actor in Russian cyber matters. However, there are other agencies involved. Heickerö described the Russian government’s cyber-related organization. Soon after Putin came

to power, Heickerö wrote, he reorganized the FAPSI (Russian acronym for Federal Agency for Government Communications and Information), often described as the equivalent of American National Security Agency. FAPSI had been responsible from 1991 to 2003 for special communications, cryptographic security, technical intelligence, counterintelligence, code cracking, telecommunications and information protection. However, in 2003, FAPSI was disbanded, with some of its assets and functions distributed among the FSB, Foreign Intelligence Service (SVR), Military Intelligence (GRU), the Federal Protection Service (FSO) and the Interior Ministry (MVD). The large portion of FAPSI that was left after the reorganization was renamed the Special Communications and Information Service and folded into the FSB (Heickerö, 2010). Former American cyber security coordinator Richard A. Clarke and co-author Robert Knake, in their 2010 book *Cyber War*, added that the FSB's 16th Directorate is believed to control Russia's reserve force of hackers (Clarke & Knake, 2010).

The FSB's 16th Directorate, explained Jeffrey Car in his book, *Cyber Warfare,* is also known as the Center for Electronic Surveillance of Communications. Carr offered another indication of the preeminence of the FSB in the cyber field. When FAPSI was disbanded in 2003, the majority of its staff was transferred to the FSB Center for Electronic Surveillance of Communications. Carr offered considerable detail about the cyber pertinent organizations internal to each of the major government agencies. Particularly useful is his catalog of Russian government IW and cyber training institutions. In sum, Carr showed that the Russian government's organization for cyber and related matters is very large and multi-faceted (Carr, 2012).

When one considers together Russia's organizational structure, the Russian definitions of strategic and operational IW, Heickerö's point about peacetime and wartime and the official

doctrine, one can see a definite military role for IW and its subset, cyber warfare. Consequently, in the Russian view, the military and the MoD would definitely play their roles. However, the Russian concept is far broader, reaching across the rest of the government to all of the assets at its disposal. It is unsurprising, therefore, to find that IW activities involve the people at the core of the aforementioned nexus of government, business and crime. Outside analysts, began linking Russia's systemic corruption to Russian government sponsored cyber activities during the 2007 attack on Estonia and 2008 attack on Georgia.

The 2007 and 2008 Cyber Attacks on Estonia and Georgia

Estonia. The proximate cause of the cyber-attacks against Estonia in 2007 was the Estonian government's decision to move a Soviet era war memorial, The Bronze Soldier of Tallinn, from the center of the capital to a military cemetery on April 27, 2007. In the early morning of April 28, Estonian government websites came under attack from a series of unsophisticated single ping denial of service attacks. Apparently, the attackers were mostly amateurs following instructions that were posted on some Russian language websites. The attacks tapered off after a few days. However, a second phase of more sophisticated attacks ensued. "The attack tools this time," wrote Heickerö, "were more sophisticated, using mainly large botnets of compromised computers conducting DDoS attacks to overwhelm information flow" (Heickerö, 2010, p. 40). Heickerö (2010) continued that the attacks appeared to have been well organized and well backed financially and intellectually.

Given the political circumstances surrounding these events, many assumed that there had been some degree of Russian government involvement, although neither the Estonian government nor anyone else in an official position straightforwardly made this accusation. However, two indications that could point to some kind of Russian government use of cyber

surrogates have emerged. First, two years after the attacks, Konstantin Goloskokov, a commissar in the Kremlin-sponsored youth group *Nashi*, told the *Financial Times* that his organization had been responsible (Clover, 2009). According to Goloskokov, he and his comrades mounted what he called a:

> Cyber defense…We taught the Estonian regime the lesson that if they act illegally, we will respond in an adequate way…We did not do anything illegal. We just visited the various Internet sites, over and over, and they stopped working. (Clover, 2009, paras. 5-6)

A second indication arose from the way in which the attacks were conducted and stopped. The Asymmetric Threat Contingency Alliance wrote, "There is evidence that Russia rented time from transnational criminal syndicates on botnets…On May 10, it appears that the attackers' time on the rented servers expired, and the botnet attacks fell off abruptly" (Thomson, 2007, paras. 6-7). At the time of the attacks on Estonia, many observers appeared unsure what to conclude. However, a year later, similar events took place in Georgia, this time, accompanied by a kinetic war.

Georgia. Throughout the world, news commentators, international relations specialists and cyber experts, who studied what had happened, directly accused the Russian government of sponsoring the attacks as their magnitude required the resources that only a state-sponsor could provide. Moreover, indicating foreknowledge of events to come, several days before the war, the website of then Georgian President Mikheil Saakashvili was subjected to a DDoS attack (Government of Georgia, 2008). Once the kinetic attack began, DDoS attacks ensued against Georgian government websites to prevent the Georgian government from getting messages to the

general population and to international media during this critical time (Government of Georgia, 2008).

With regard to the attacks on Georgia in 2008, one should review the research conducted by the US-CCU (US-CCU, 2009). The findings concluded that cyber-attacks were an integral part of Russia's armed attack on Georgia:

> The organizers of the attacks had advance notice of Russian military intentions, and they were tipped off about the timing of Russian military operations…Many of the cyber-attacks were so close in time to the corresponding military operations that there had to be close cooperation between people in the Russian military and the civilian cyber attackers. (US-CCU, 2009, p. 3)

Moreover, the US-CCU report indicated that most of the botnets, Internet Protocol (IP) addresses, and autonomous systems used against Georgia had already been used for criminal activities. Indeed, some of them even took breaks from the war to launch criminal operations (US-CCU, 2009). An illustration of how journalistic accounts can help with this kind of multi-disciplinary analysis is provided by a *New York Times* article that appeared just after the 2008 conflict, that is, before the US-CCU report was published. In it, Don Jackson, Director of Threat Intelligence for SecureWorks, presaged the US-CCU report not only by attributing the cyber-attacks against Georgia to criminals, but by naming the specific criminal group—Russian Business Network, frequently referred to as the RBN (Markoff, 2008, August 12, para. 14). Although RBN appears to have dissolved as a single criminal entity, IP addresses and autonomous systems associated with this group have reappeared in the case of the Georbot espionage malware, discussed below (Akhvlediani, 2012). RBN was also a prime suspect in a 2008 attack on the U.S. Pentagon and Treasury Department's computer networks (Flook, 2009).

The perpetrators of the cyber-attacks on Georgia formed a trichotomy. The real leaders, that is, those who were privy to at least some of the government's war plans against Georgia, operated from a distance. There was a hierarchy to the actors involved: at the top were professional planners, computer scientists and engineers. Next, in the middle of the trichotomy, were criminal organizations paid to carry out certain elements of the attacks. There were indications implicating RBN (Mshvidobadze, 2009). RBN was a group of cyber criminals with ties to Russian President Vladimir Putin (Corbin, 2009). Lastly, there were volunteers, individuals with PC's who were recruited through social networks to augment the attacks (Mshvidobadze, 2009).

In *Project Grey Goose Phase I Report* (Project Grey Goose, 2008), Jeffrey Carr, author of *Cyber Warfare,* focused on these amateur attackers. They were recruited to carry out cyber-attacks on Georgia through websites like xaker.ru and stopgeotgia.ru. Carr's group of experts studied posts on these two sites as well as network log files from 149 Georgian websites. From this data, they constructed the likely kill chain: encourage computer novices with patriotic appeals, publish a target list, select malware for use, launch the attack and evaluate results. Unlike the US-CCU report, Grey Goose does not examine the other, more professional, aspects of the cyber-attacks on Georgia, nor does it attempt to determine who was behind the recruitment of the novice hackers (Project Grey Goose, 2008).

The US-CCU report said that some of the website defacements were carried out by Structured Query Language (SQL) injections by which hackers break into a site by exploiting security vulnerabilities in the database layer of an application. The hacker is then able to communicate directly to the database. This injection mechanism is frequently used by cyber criminals to steal data from the target. For example, it can read, remove, add and change data.

This method can change the site's usual appearance and hackers can post information that benefits their purpose. The system administrator is helpless to maintain and execute command and control over the server. To counter this, some Georgian websites were re-hosted on servers in Estonia and the United States (US-CCU, 2009).

Interestingly, the attacks directed against Georgia represented a considerable improvement over those directed just one year earlier against Estonia. DDoS attacks on Estonia were based on Internet Control Messages Protocol (ICMP), which is the Internet protocol that generates error messages when one seeks a non-existent web-site. The attacks directed against Georgia involved Hypertext Transfer Protocol (HTTP) packages that placed greater demands on the attacked servers. The US-CCU writes:

> Most of the cyber attack tools used in the campaign appear to have been written or customized to some degree specifically for the campaign against Georgia. The tools employed for denials of service included three different software applications designed for 'stress tests' in which web servers are flooded with HTTP packets to see how much of this traffic they can handle. A fourth piece of software was originally designed for adding functions to websites, but was adapted by the attackers so that it would request random, non-existent web pages. These HTTP-based attack tools were tested by the US-CCU in a laboratory environment and proved far more effective than the ICMP-based attacks that the Russians had used in Estonia. (US-CCU, 2009, p. 4)

Complementing the Grey Goose report, the US-CCU report pointed out that there were web postings of instructions to individuals with limited computer skills who could contribute to the cyber-attack efforts. The web-site postings were so productive that 43 targeted websites were

effectively shut down or defaced, in addition to the eleven targeted by the botnets associated with organized crime. Social networks and websites such as stopgeorgia.ru and stopgeorgia.info were used to recruit and prepare such hackers for action. The US-CCU report noted that the social networking sites employed were not those dedicated to computers or hacking, but the familiar ones dedicated to personal information, dating, hobbies, etc. In contrast, the stopgeorgia websites were sites dedicated to attacking Georgia. These provided lists of suggested Georgian target sites and provided information on how to do it. These sites were hosted on servers in the U.S., Germany and Latvia with already established ties to organized crime (US-CCU, 2009).

The link to specific elements of organized crime, of course, comes from forensic analysis and from interviews and research. Consequently, one must again turn to some research institute and journalistic sources to fill in some of the gaps. Researchers apart from the US-CCU concluded that the criminal involvement in the attacks on Georgia was largely by RBN. The principles of RBN were believed to have close ties to the Russian government. In particular, one RBN principal, Aleksandr Boykov, is a former lieutenant colonel in the FSB. RBN was an Internet service provider in Russia until 2007 and was involved in various aspects of criminality such as phishing, malware distribution, malicious code, botnets, DDoS attacks and child pornography. Some experts believed that RBN was also involved in the cyber offense against Estonia. François Paget, senior expert for the McAfee Company, for example, says RBN was behind the cyber-attack on Estonia (Flook, 2009). Russian government collusion with cyber criminals is a cost-effective way to maintain state-of-the-art capabilities and to capitalize on the American and West European countries' emphasis with attribution to courtroom standards (Thomson, 2007, para. 6).

Another indication of official Russian involvement in the cyber-attacks on Estonia and Georgia comes from well-sourced bloggers. Such writers are more important in Russia than they are in western countries because they are the only independent internal sources of information in Russia. Anton Nossik is a close observer of cyber developments in Russia and Media Director at the international media company SUP, which owns LiveJournal. After a series of cyber-attacks against Russian domestic political opposition websites, he wrote:

> It is important to understand that here we are dealing with a well-established business with an impressive turnover and solid state backing and financial support. DDoS-attacks, hacking blogs and e-mails - it's their old, common business. At first glance, just look whom our [Russia's] elusive and omnipresent cyber crime targeted over the years and then the main principle of this list will be clear. We will see in it [the list of attacked sites] websites of Georgian and Estonian government agencies, servers of Kommersant and Gazeta.ru [newspapers] and opposition blogs…In one day, the Georgian blogger Cyxym's LiveJournal, FaceBook and Twitter [pages] were taken down…It is difficult to imagine a single customer for all of these cyber vandalism acts…Suffice it to recall the history of the organization in Russia with an almost unpronounceable name: Interregional Public Organization Promoting Sovereign Democracy, the youth movement Nashi. (Nossik, 2011, paras. 4, 6)

Nossik combined the 2007 and 2008 cyber-attacks on Estonia and Georgia with the similar tactics employed against domestic political opposition during the months preceding the 2011 Duma elections and the 2012 presidential election to present a syndrome of Russian government-sponsored cyber-attacks.

Ukraine 2013-2014

Some have been tempted to show that the syndrome extended into the 2013-2014 Russia-Ukraine conflict. There have been similarities, however, a closer look also revealed important dissimilarities. Because, at the time of this writing, the conflict is ongoing, there has been little time for analysts to step back and develop a full and accurate account of what has happened. Smith (2014b) and Giles (2014) take steps in that direction, however, their work must be complemented by journalistic accounts, security company publications and the work of individual cyber security researchers such as Glib Pakharenko (2014). Pakharenko has attempted to show what has been going on in his country, Ukraine, with a PowerPoint presentation that he has made at some international conferences and shared with colleagues, including this author.

Although some elements of the press tried to promote the idea of cyber war with headlines such as "Russia and Ukraine in cyber 'stand-off'" (Lee, 2014) or "The Ukraine-Russia cyber war is heating up" (Bender & Kelley, 2014), the reality has been more subtle and complex. Pakharenko explained the major technical difference between Georgia in 2008 and Ukraine in 2014 was that Ukraine had a much more developed Internet infrastructure:

> The main UA-IX [Ukrainian Internet exchange] has main routes and re-routing to and from RU [Internet domain abbreviation for Russia], but has strong existing routing to E.U. based IXs. This added EU routes may well have prevented or should prevent UA [Internet domain abbreviation for Ukraine] from being overwhelmed [sic.]. (Pakharenko, 2014, Slide 13)

In 2008, 90% of Georgia's Internet traffic passed through Russia (Smith & Mshvidobadze, 2011, p. 3). Even today, Georgia has no Internet exchange points while Ukraine has six (Smith, 2014b). Moreover, Ukraine has a well-developed human infrastructure. Ukraine ranks fourth in the world

in number of certified information technologists, behind India, the U.S. and Russia, and many American and European information technology companies sub-contract with Ukrainian organizations (Software development, 2008, p. 2).

The combined effect of many qualified people on all sides, target-rich environments in both Russia and Ukraine and at least adequate defenses on both sides resulted in what Smith calls "tit-for-tat hacker attacks" (Smith, 2014b). Attribution has been hard to establish, and ultimate responsibility even more so. As Pakharenko pointed out, "When the war between Russia and Ukraine has started, several 'anonymous' groups were created, e.g. 'CyberBerkut' in support of Russia and 'Cyber 100' in support of Ukraine [sic.]" (Pakharenko, 2014, Slide 2). As in the cases of Estonia and Georgia, some indications of criminal links to some attacks have been established. For example, Internet security companies Dell Secure Works and Arbor Networks detected the use of banking Trojans DirtJumper and Drive in attacks against Ukrainian government sites (Brewster, 2014). Moreover, out of all the apparently pro-Russian and apparently pro-Ukrainian attacks, Smith assessed that three had clear strategic purpose, that is, that their timing coincided with some major geopolitical event: February 28-March 3, when the Russians invaded Crimea; March 16-17, when a referendum on Crimea joining Russia was conducted; and just before May 25, when the Ukrainian presidential election took place (Smith, 2014b). Nonetheless, no author has yet said definitively that either the Ukrainian or Russian government has been behind any of the attacks.

There are two other factors that have further confused examinations of what has been happening in Ukraine. First, many physical attacks were reported in the press as part of the presumed cyber war. Pakharenko goes so far as to say that physical attacks have had the largest impact (Pakharenko, 2014). Under the headline "Cyber war with Russia heating up," one

journalist explained that "A group of unidentified men took control of several communications centres in Crimea…They wrecked cables, knocked out almost all landline, mobile and Internet services in the region" (Russon, 2014, para. 2). Meanwhile, Ukrainian parliamentarians experienced difficulties with the cellular telephones, allegedly because the Russian security services had inserted some kind of device on the equipment of Ukrtelecom in Crimea.

The second confusing factor has been that social media have been used by all sides to spread their own narratives, to organize demonstrations and recruit volunteers. Understandably, this has created an impression of conflict, however, it would be imprecise to call it cyber conflict. For example, On March 3, the Russian Internet regulating agency, Roskomnadzor, ordered social media giant VKontakte to block 13 pages that published pro-Ukrainian content (Rahn, Khrennikov & Eglitis, 2014, para. 15). This action was part of Russia's ongoing effort to control content on the Internet, exacerbated by the conflict with Ukraine, but it was not a cyber-attack.

Of course, there have been many cyber-attacks in the Russia-Ukraine conflict, and further analysis may reveal that some of them should be attributed to the Russian security services or their criminal associates. However, one must conclude that cyber warfare has not been as big a factor as it was in the 2007 and 2008 attacks on Estonia and Georgia. Making sense of what has happened requires recollection of the point made above that the Russians think in terms of IW, of which cyber warfare is just one part, and that IW is constant, in peace and war. Giles wrote that while many incidents have been reported in the west as cyber-attacks, "In Russia they fall under the much broader category of 'information warfare.' This is a wide-ranging, holistic area of offense activity by the state which encompasses far more than technical cyber exploits" (Giles, 2014, para. 4).

Cyber Espionage

Furthermore, Giles offered the example the espionage malware Uroburos or Snake — as a phenomenon that was improperly reported as part of cyber warfare in the 2014 Russia-Ukraine conflict:

> In fact, [Snake] is a long-standing exploit whose deployment dates back at least four years, with some elements of the software created as long ago as 2005…Thus Snake is not a result of the conflict between Russia and Ukraine; it's a precursor to it. Cyber espionage is a crucial part of positioning for Russian foreign policy in former USSR countries. Accessing the information systems of diplomatic, government and military organizations over many years gives Russia a huge advantage in predicting the tactics and thinking of its neighbors. (Giles, 2014, paras. 8-9)

The press's confusion over Snake/Uroburos/Turla arose from misunderstanding the nature of this malware but also from the timing of two major reports about it. Both were issued at the height of the Russia-Ukraine conflict. On March 1, 2014, G Data published its report (Uroburos, 2014) and on March 8, BAE Systems published its report (Snake 2014). Snake is sophisticated espionage malware that has been operating since at least 2011. It can steal files and capture network traffic. The G Data analysts argued that, given its complexity, it is likely the product of a nation-state's security service, apparently written by Russian speakers who work in the UTC+4 time zone, that is, Moscow's time zone.

Moreover, the G Data analysts wrote, Snake is related to Agent.BTZ, which was used to attack U.S. targets, including the U.S. Department of Defense, in 2008. They offered three pieces of evidence to support this claim. First, when Snake gains access to a computer, it checks for the presence of Agent.BTZ and remains inactive if it is present. Second, Snake and Agent.BTZ use

the same obfuscation key. Third, both use the same file name to store logs (Uroburos, 2014). The BAE Systems report indicated that Snake had existed since 2005. It did not implicate the Russian security services as strongly as the G Data report, noting only that work on this malware had been accomplished in the UTC+4 time zone. On the relationship between Snake and Agent.BTZ the two reports are in agreement (Snake, 2014).

This links apparent Russian cyber espionage against neighboring countries to apparent espionage against the United States, which underscores a finding of the U.S. National Counterintelligence Executive:

> Motivated by Russia's high dependence on natural resources, the need to diversify its economy, and the belief that the global economic system is tilted toward U.S. and other Western interests at the expense of Russia, Moscow's highly capable intelligence services are using HUMINT, cyber, and other operations to collect economic information and technology to support Russia's economic development and security, points out U.S. National Counterintelligence Executive. (U.S. National Counterintelligence Executive, 2011, p. 5)

The discovery of Georbot, another piece of espionage malware apparently traceable to the Russian security services, further underscores Giles's point about the enduring importance to Russia of espionage against its neighbors. Computer Emergency Response Team (CERT) of Georgia discovered Georbot in March 2011. The Georgian CERT's investigation was carried out in concert with the U.S. Federal Bureau of Investigation (FBI) and Department of Homeland Security, German, Polish and Ukrainian CERTs and security companies from Europe and the U.S. Georbot was sophisticated espionage malware, spread first by watering hole attacks and later by phishing. In the watering hole attacks, popular Georgian news portals were infected.

Anyone who visited one of these news sites and entered a security-related key word, in English or Georgian, was infected. Georbot was able to steal files and credentials, take screenshots, record audio and video and find network hosts. It reported back to a series of command and control servers that passed their functions off to another server upon discovery. The IP addresses and Domain Name System (DNS) servers were previously associated with the criminal group RBN. After the command and control servers had all been exhausted, Georbot was spread by spamming. CERT-Georgia traced the origin of the spam messages through an obscure Indian WHOIS to Lubyanka 13 in Moscow, the Information and Communications Technology Division of the FSB. With help from the FBI and other friendly country agencies, CERT-Georgia reverse engineered Georbot, infected a document that contained appropriate key words and discovered the author of the malware, a known Russian hacker with ties to the Russian security services (Akhvlediani, 2012).

Another piece of malware used for an espionage campaign that originated in Russia is Gyges, discovered by Sentinel Labs in March 2014. Gyges was discovered not in the national security computers of a nation-state, but in use with common criminal malware such as Cryptologger. Nonetheless, Sentinel Labs analysts assessed that Gyges is government-grade espionage malware because of its capabilities, the resources that must have gone into it and because components of its code match components of the codes of known espionage malware. The attraction to cyber criminals, Sentinel Labs suggested, is the superior evasion capabilities that Gyges affords. “Gyges is an early example of how advanced techniques and code developed by governments for espionage are effectively being repurposed, modularized and coupled with other malware to commit cyber crime” (Peters, 2014, para. 2). In a western country, one might wonder how a piece of sophisticated government espionage malware came into the hands of

criminals. However in Russia, where cyber criminals figure prominently in state matters, it is unsurprising that state assets sometimes figure prominently in criminal matters.

Diplomacy as Part of Information Warfare

Given the importance in Russian thinking of IW, of which cyber is a subset, and the way that the nexus of government business and crime operates, it is understandable that the Russian government is anxious to protect its assets and its secrets. Recalling that IW is a continuous effort, in wartime and peacetime, one should understand that Russia's diplomatic efforts are also part of its information strategy. Consequently, one must review Russia's relevant activities in the international arena. Although Russian diplomats often speak about some sort of agreement to prevent cyber offenses, Moscow has refused to sign the only extant document with any promise of efficacy, the *European Convention on Cyber-crime,* open for signature since 2001 (Convention on Cybercrime, n.d.). Vladislav Sherstuyuk, a retired general who heads the Institute of Information Security Issues at Moscow State University and sits on Russia's National Security Council, explained Russia's position: "Russia wants to preserve state sovereignty and monopoly on the conduct of investigative activities based on existing domestic laws and procedures" (Talbot, 2010, para. 5). This stance minimizes the possibility that any other country will be able to garner hard evidence of exactly how the nexus of government, business and crime works in cyber matters.

However, Moscow has a treaty proposal of its own. It has been advocating at the United Nations General Assembly a revised version of a Shanghai Cooperation Organization *Agreement on Cooperation in the Field of International Information Security.* The thrust of the agreement is to outlaw the broadcast by mass media or across the Internet of any information that could "distort the perception of the political system, social order, domestic and foreign policy,

important political and social processes in the state, spiritual, moral and cultural values of its citizens" (Agreement, 2008, para. 2[5]). States should monitor and censor information to insure security and stability (Agreement, 2008).

Furthermore, each year since 1998, Russia has introduced a resolution at the United Nations (U.N.) calling for an international agreement to combat what it calls information terrorism. At the U.N. Committee on Disarmament in 2008, Sergei Korotkov of the Russian Defense Ministry, argued that anytime a government promotes ideas on the Internet with the goal of subverting another country's government - even in the name of democratic reform - it should qualify as aggression, which would make it illegal under the prospective treaty (Gjelten, 2010).

Summary of the Literature Review

The literature on how corruption and geopolitics in Russia combine to nurture multiple cyber threats to Russia's neighbors and to the U.S. is extensive and eclectic. However, it may be stronger because different people, with different roles and perspectives have examined different aspects. The picture that emerges from a review of their work is one of systemic corruption presided over by President Vladimir Putin, with the *siloviki* playing a major role in every aspect of the system. The systemic corruption skews normal economic development and concentrates what wealth there is in the hands of a few. Meanwhile, the educational system that Russia inherited from the Soviet Union continues to produce people who excel at math and science. With poor job prospects, some of these people are attracted to crime, particularly cyber-crime. In the environment of systemic corruption run by the *siloviki,* cyber criminals can thrive, so long as they do not harm the interests of the oligarchy or the interests of Russia, as the *siloviki* perceive those interests. In this context, their skills fit very well into a well-developed doctrine of IW. Consequently, some amount of cyber-criminal time and resources is dedicated to Putin's

geopolitical agenda. IW, and more specifically cyber techniques, are used to control information, commit espionage and attack neighbors directly.

Of course, the immediate impact of this is directed at Russia's immediate neighbors, the countries of the former Soviet Union and the Warsaw Pact, however, it also affects U.S. interests. Because most of the Russian narrative is anti-American, allowing Russia to control information in Eastern Europe and Central Asia runs counter to American interests. Moreover, the U.S. has formal alliances with many of the countries involved and an informal alliance with Georgia. Consequently, some actions against those countries could also impinge on U.S. security interests. Finally, as shown by the relationship of Uroburos/Snake/Turla to Agent.BTZ, Russia's cyber espionage also directly targets America. In sum, the sociology, politics and economy of contemporary Russia is producing cyber threats to its neighbors and to the U.S.

Discussion of the Findings

The purpose of this research was to examine how certain systemic characteristics of contemporary Russia, including its political economic and social systems, have promoted multiple cyber threats to neighboring countries and to the U.S. The utility of this study is that it may help to inform the American foreign policy public about this important matter. The research answered the following questions: What is the Russian approach to IW and its subset, cyber warfare? How is Russia's doctrine on IW tied to its geopolitical ambitions? What is the relationship between the Russian government and Russian cyber criminals in this regard? Does Russian cyber espionage pose a threat to neighboring countries such as Ukraine and Georgia and to the United States? Research into these questions must touch upon computer forensics, military strategy, geopolitics, current events and recent history, politics, economics and sociology.

Consequently, it must review a multi-disciplinary collection of literature. It was a challenge to collect representative, unbiased literature that could be examined within a reasonable period.

The Russian cyber threat is often overlooked and should be better understood. Russian cyber capabilities and activities pose threats to its neighbors, that is, the countries of the former Soviet Union and some of the Warsaw Pact, and to the U.S. Of course, there have been many studies that have looked at various aspects of Russian cyber capabilities and activities, however, none has sought the root causes of Russia's approach. This study attempted to answer whether systemic corruption in Russia combines with Russia's current geopolitical aims to produce a threat to Russia's neighbors and to the U.S., which is poorly understood by Americans, possibly because of different approaches to the subject.

The evidence of corruption in Russia is overwhelming and accumulating every day. At the moment of this writing, the *New York Times* detailed how the textbooks for Russian schools have been purged on a variety of political and bureaucratic pretexts. In some cases, the Russian Ministry of Education eliminated textbooks because their publishers had made an error in submitting the paperwork. In another, an official objected to using foreign cartoon characters to teach math. Some of the *Times's* article is worth repeating:

> There was, however, one standout winner: a publishing house whose newly appointed chairman was a member of President Vladimir V. Putin's inner circle. Arkady R. Rotenberg, a judo sparring partner from Mr. Putin's St. Petersburg youth…Mr. Putin first directed that the state-owned company be sold into private hands, records show, in a deal that circumvented a requirement intended to ensure the highest prices for state assets. Then, having installed Mr. Rotenburg as chairman, Mr. Putin's government knocked out much of Enlightenment's competition. (Becker and Myers, 2014, November 1)

This one account illustrates three points. First, stories like this occur frequently. Second, corruption in Russia pervades every aspect of life. Third, corruption in Russia is directed from the top, that is, by Putin.

However, the challenge for this study was not to find corruption in Russia, but to present it in political science terms that are meaningful to a study of how a country's political, economic and social system works. Elaine Byrne's work established some criteria for different types of corruption. Byrne was chosen because she offered straightforward definitions and because, as an adviser to the E.U., she has practical experience in examining how certain contemporary polities work. Her distinction between systemic corruption and petty and sporadic corruption is essential because a critic might argue that there is corruption everywhere. This is true, but systemic corruption is corruption that pervades the entire political, social and economic system (Byrne, 2009).

The next challenge was to establish that contemporary Russia matches Byrne's description of systemic corruption. There are many articles, books and other materials that look at different aspects of corruption in Russia. One might have chosen *Putin's Russia: Life in a Failing Democracy* by journalist Anna Politkovskaia, assassinated in her apartment building elevator in 2006 before she was to have published her investigation of Russian army misconduct in Chechnya (Politkovskaia, 2007). Or one might have used as illustrations some recent high profile cases, for example, examining the materials accumulated by the U.S. Congress as it considered sanctions against Russia after the 2009 death of lawyer Sergei Magnitsky while in FSB custody. By imposing sanctions on Russia in the wake of the Magnitsky case, the U.S. Congress implicitly pointed at systemic corruption in Russia; it would not have imposed sanctions on an entire country for a singular instance of corruption. Even the law's formal

name—Sergei Magnitsky Rule of Law Accountability Act—implies systemic corruption (Lally and Englund, 2012). There are many more potential sources, however, they all agree that Russia is characterized by systemic corruption.

Felshtinsky and Pribylovsky (2008) and Satter (2003) are representative for three reasons. The first reason was to gain the advantage of the different perspectives of Russian authors who have studied the power structure in their country and of a foreigner who knows Russia well. The second reason was that these two books did not focus on a single instance of systemic corruption, but at wide ranges of accounts. Third, both the Russian and the American authors offered analytical explanations aimed at readers in the U.S. and the countries of Western Europe.

Satter explained that the systemic corruption in Russia is a legacy of a rush to capitalism without rule of law. In such a system, there is money, but only the rule of the rich and powerful, that is, class of people that Felshtinsky and Pribylovsky call oligarchs. The Russian co-authors explained that the *siloviki* play a key role in Russia's systemic corruption, broadly penetrating government agencies and businesses. They are inclined toward state intervention in the economy in cases of national security, as they perceive it (2008).

From that point, it was necessary to focus specifically on cybercrime in Russia. With this, too, there is no lack of material. Most of it is anecdotal, that is, journalistic accounts of how a piece of malware of Russian origin worked and how it was discovered, or technical, that is, the detailed analysis of such malware by security firms. There is no prominent literature to suggest that cyber-crime of every sort is not prevalent in Russia. Goncharov's Trend Micro study was chosen because it catalogs Russian involvement in every aspect of cyber-crime. Goncharov performed an important service by researching and presenting all this material together because individual accounts do not have the same effect on a reader. However, Goncharov's work must

be combined with another observation to illustrate how cyber-crime in Russia is part of the systemic corruption.

In this researcher's experience, finding extensive criminal activity on the Runet, as Russians colloquially call their portion of the Internet, is not difficult. The FSB, MVD and other security agencies can easily find it. Nonetheless, criminal websites persist despite constant monitoring by SORM-3, an Internet and communication device monitoring system that collects and stores information (SORM 3, n.d.). Such websites also persist despite the Russian government's efforts to shut down websites that it determines are unacceptable. The logical conclusion is that criminal websites, or at least many of them, are not unacceptable to the Russian government.

Another point that emerges from Goncharov's comprehensive approach is that there are many talented people available to Russian cyber-crime. Smith (2014b) explained that this is because there is a high level of education in Russia contrasted with a low level of opportunity. Consequently, some very qualified people turn to crime.

Russian systemic corruption pervades everything, including cyber-crime. Moreover, given the central role of the *siloviki,* it is reasonable to assume that cyber-criminals are drawn into national security matters, as defined by the *siloviki.* Here it is important to recall Felshtinsky and Pribylovsky's point that the *siloviki* generally believe in state intervention in the economy for national security purposes (Felshtinsky & Pribylovsky, 2008). However, a stronger link between cyber criminals and Russia's current geopolitical activities would be established if it can be shown that cyber warfare has a place in Russian governmental doctrines, particularly a doctrine that extends beyond the strictly military realm.

What is the Russian Approach to Information Warfare and its Subset, Cyber Warfare?

Apart from journalistic pieces that appear each time a Russian official mentions the possibility of a military cyber command, only three people have achieved expertise in this area. Consequently, this study relied heavily on Heickerö (2010), Thomas (1996 & 1996-1997) and Giles (2011 & 2014). Together, they show that, in the view of the Russian government, cyber warfare is a tool of IW. Russian thinking about IW dates to the writings of respected Soviet military theorists and has been well developed since the 1980s.

The writings of these three experts underscore two aspects of the Russian approach to IW that may be unfamiliar to western observers. The first aspect is that the Russians have a broad approach to IW, which includes cyber warfare, but also includes intelligence, counterintelligence, *maskirovka*, (making things appear what they are not) disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure and destruction of enemy computer networks and software applications (Thomas, 1996-1997).

This enables the Russians to select the right mix of tools for the job. In Estonia in 2007, they combined cyber war with political subversion; in Georgia in 2008, they combined cyber war with kinetic war; in Ukraine in 2014, they combined political subversion, kinetic war and a more general information war (Giles, 2014). This not only enables the Russians to optimize their mix of tools for the geopolitical situation, it also confuses many western observers as evidenced by headlines such as "Russia and Ukraine in cyber 'stand-off'" (Lee, 2014).

The second aspect of the Russian approach to IW that may be unfamiliar to some western observers is its persistence. IW takes place 24 hours a day, 7 days a week, 52 weeks a year, in wartime and in peacetime (Thomas, 1996-1997). The implication of this finding is that Russia is

right now waging some kind of IW against the countries that it perceives as adversaries. There is no point inserting the adjective potential before the noun adversaries, as some westerners might do. According to the Russian doctrine, IW is constant, not triggered by some event that makes a particular country an adversary of Russia. Put another way, Russia has perpetual adversaries. Russia's neighbors, that is, the countries of the former Soviet Union and some of the Warsaw Pact, and the U.S. should assume that Russia is carrying out some form of IW against them.

Cyber espionage, which will be discussed below, is an obvious manifestation of this aspect of Russian IW doctrine. However, there may be others. In this regard, Symantec's report on Energetic Bear, also known as Dragonfly is important. Symantec described Dragonfly as an ongoing cyber espionage effort that has been underway at least since 2011. Dragonfly initially targeted defense companies, but then shifted its focus toward energy companies and the companies that make ICSs for the energy industry (Symantec, 2014). This is a cause for concern as the gathering of information about U.S. energy industry ICSs and the manufacturers of such ICSs could indicate planning to move beyond espionage to computer network attack.

How is Russia's doctrine on information warfare tied to its geopolitical ambitions?

It is important to note that senior Russian officials were speaking about IW substituting for kinetic weapons by the mid-1990s. Recall the words of General Samsonov, cited by Heickerö (2010). In the Russian view, IW could be used to disrupt state administration, hit strategic targets and affect the spirit of the population. It is, furthermore, important that the substitution of information weapons for kinetic weapons appeared as official policy in Russia's 2010 military doctrine (Russian Federation, 2010). These statements reflect a Russian view that has been held for two decades that IW is tied to the country's geopolitical aims. The 2007 incidents against Estonia may have been an attempt to achieve coercive political objectives with IW, particularly

cyber weapons, without the use of kinetic weapons. The 2008 attacks on Georgia appear to have been an attempt to substitute such weapons for some, although not all, kinetic weapons.

What Is The Relationship Between the Russian Government and Russian Cyber Criminals with Regard to Geopolitical Ambitions?

There were indications of Russian government collusion with cyber criminals in the 2007 cyber-attacks on Estonia. First was the admission of a *Nashi* commissar (Clover, 2009). Second was that the way the second wave of attacks were conducted. On May 10, 2007, the attacks abruptly ended, suggesting the use of rented botnets. (Thomson, 2007).

A year later, Russia and Georgia fought the first ever combined kinetic and cyber war. There were hundreds of articles written on this subject, however, there were three major studies that furthered understanding of what had happened. The author principally relied on the US-CCU because it was conducted by an independent organization, it was comprehensive and it applied multi-disciplinary information in its analysis (US-CCU, 2009). The Grey Goose report was also very good, however, it was less comprehensive than the US-CCU report and, with regard to the recruitment of amateur hackers, corroborated the findings of the US-CCU.

The third study was *Russian Invasion of Georgia: Russian Cyberwar on Georgia* (Government of Georgia, 2008). This was a good report to which this author contributed, however, it was prepared and published by the Georgian government. Consequently, some could question its objectivity. Therefore, the author relied upon this study only to establish the fact of the last, that is, August 27, DDoS attack of the 2008 war. Moreover, the paper is useful because it records the official Georgian government position, tracing the cyber-attacks to July 19, 2008, two weeks before the kinetic attack, to August 27, 2008, well after the ceasefire (Government of Georgia, 2008).

The US-CCU report made two important breakthroughs. First, rather than analyzing only computer logs, it combined technical analysis with geopolitical analysis. In that context, it carefully matched the timing of cyber events to the timing of kinetic military events. The US-CCU analysts agreed that the attackers were civilians, however, their methodology allowed them to conclude that someone who was coordinating the cyber-attacks was privy to Russian military plans. This links Russian cyber criminals to the geopolitical purposes of the Russian state. This is an important breakthrough because until the US-CCU report, many observers in the U.S. and the E.U. had been searching in vain for evidence of direct Russian government involvement.

The second breakthrough in the US-CCU is to tie the botnets, IP addresses, and autonomous systems used against Georgia to those that had already been used for criminal activities (US-CCU, 2009). Other analysts explicitly identified the criminal RBN as the focal point of the cyber attacks directed at Georgia as part of the 2008 war (Markoff, 2008). One of the principals of RBN was Aleksandr Boykov, a former lieutenant colonel in the FSB (Flook, 2009).

Although the kinetic portion of the 2008 Russia-Georgia war ended in a ceasefire and Russian occupation of two Georgian regions, the geopolitical rivalry between these two countries persists, as does Russian cyber espionage against Georgia. The 2011 discovery of Georbot provided another indication of criminal involvement in the geopolitical purposes of the Russian state. RBN appears to have dissolved as a single criminal entity sometime in 2008. Nonetheless, the Georgian CERT was able to link some of the IP addresses and DNS servers associated with Georbot with some of those associated with RBN in 2008 (Akhvlediani, 2012).

One final indication of a link between the Russian state and cyber criminals comes from espionage malware known as Gyges. Sentinel Labs, which discovered Gyges, assessed that it is government-grade espionage malware with some code components that match code in previously

known espionage malware. In this case, it appeared that criminals borrowed a government asset to use in ransomware like Cryptolocker (Peters, 2014). Given the degree of apparent collusion between cyber criminals and the Russian government, the appearance of Gyges in conjunction with purely criminal malware is unsurprising. Nonetheless, if this occurrence develops into a trend, one can expect ever more potent criminal malware.

These observations lead directly to the twofold value of this study. First, this study methodically built the context in which Russian cyber criminals and the Russian government collude on affairs of state. Second, this study explained the political, economic and social reasons for this phenomenon. These are important contributions because they run counter to the experience and expectation of most observers in the U.S. and Western Europe. This may be because most of these people are familiar with what Byrne calls petty and sporadic corruption, not systemic corruption as it has developed in Russia.

Does Russian Cyber Espionage Pose a Threat to Neighboring Countries Such as Ukraine and Georgia and to the United States?

Unlike systemic corruption, espionage is better understood by observers in the U.S. and Western Europe. As Giles pointed out, the 2013-2014 Russia-Ukraine conflict has been one more of IW than cyber war, despite some headlines in the popular press. Also despite some headlines, Uroburos/Snake/Turla is a long-standing cyber espionage effort against Ukraine and, to a lesser extent, against Lithuania, not an attack directed at Ukraine as a result of the 2013-2014 conflict (2014). At approximately the same time, the Georbot virus was deployed against Georgia. In the case of Georbot, this study referred to the only report containing primary research, the report of the Georgian CERT (Akhvlediani, 2012). In the case of Uroburos, the author again referred to the only literature that contained primary research data, that is, the

literature published by the two Internet security companies that analyzed Uroburos. These reports were consistent with each other about Uroburos, including the observation that it is related to Agent.BTZ (Snake, 2014; Uroburos, 2014).

The finding about the Uroburos connection to Agent.BTZ leads to another contribution of this study, which is to point out that the link between Uroburos and Agent.BTZ links Russian espionage against neighboring countries to espionage against the U.S. In his 2010 *Foreign Affairs* article, former Deputy Secretary of Defense William Lynn called the 2008 Agent.BTZ attack "The most significant breach of U.S. military computers ever" (Lynn, 2010, para. 2). At the time, Lynn attributed the attack only to a foreign intelligence service; however, the revelation about the relationship between Uroburos and Agent.BTZ provides a strong indication that it was a Russian intelligence service.

The results of this study with regard to espionage connect three of the four questions posed. RBN, or whoever has taken control of RBN's assets appears to play a pivotal role. The Georgian CERT has connected Georbot to RBN (Akhvlediani, 2012). Other analysts have linked RBN to Agent.BTZ (Flook, 2009). More recently, a number of Internet security companies have linked Agent.BTZ to Uroburos (Apps and Finkle, 2014; How Turla, 2014; Snake, 2014; Uroburos, 2014). Finally, RBN has been identified as a cyber-criminal syndicate with ties to Putin (Corbin 2009). These are strong indications that the Russian state colluded with the criminal RBN to mount major cyber espionage campaigns against neighboring countries and against the U.S., and that a similar relationship persists between the Russian state and the successor or successors to RBN.

Four major themes emerged from this study. The first theme is that the dominant characteristic of the Russian polity is systemic corruption presided over by President Vladimir

Putin, in which the strongest element are the *siloviki.* The second theme follows from the first. Because everything is based upon corruption, there is a unique Russian nexus of government, business and crime in which there is collusion on everything. It is unsurprising, then, that there is collusion among government, business and cyber criminals. The third theme is that this collusion fits into a long-standing and well thought out doctrine of IW, which includes cyber. Putting the first three themes together, cyber criminals have become an asset in furthering Russia's interests abroad, as defined by Putin and the *siloviki.*

This study developed a new approach to such problems by combining the traditional emphasis on computer forensics with military strategy, geopolitics, current events and recent history, politics, economics and sociology. This yields a more accurate context from which to understand what is actually happening in Russia. Although the details would differ, one could easily use this methodology to understand cyber activities in other countries. Moreover, a number of questions for further research emerged from this study. These will be discussed in the Future Research and Recommendations section.

Future Research and Recommendations

The fundamental problem that this study addressed is that the Russian cyber threat is often overlooked and should be better understood. The study unequivocally established that contemporary Russia is characterized by systemic corruption, presided over by President Vladimir Putin, with the *siloviki* playing a major role in every aspect of the system. In the environment of systemic corruption run by the *siloviki,* cyber criminals can thrive, so long as they do not harm the interests of the oligarchy or the interests of Russia, as the *siloviki* perceive those interests. However, Putin and the *siloviki* are not solely interested in criminal enterprise; they are also interested in advancing Russia's geopolitical interests, as they perceive them.

Consequently, some amount of cyber-criminal time and resources is dedicated to Putin's geopolitical agenda. IW, and more specifically cyber techniques, are used to control information, commit espionage and attack neighbors directly. Because this runs counter to the expectations of most Americans, a number of national level recommendations emerge from this study.

Moreover, this study had two limitations. First, it opened the door to a vast field of endeavor, namely Russian cyber capabilities, military strategy, geopolitics, politics, economics and society. This was necessary to explain the Russian cyber threat fully. However, it also means that it leaves many areas yet to be fully explored. Second, this study was constrained both in time and space. As a consequence of these two factors, a number of suggestions for further study emerge. A number of national level action recommendations is indicated.

At the outset of this paper, the author quoted U.S. Director of National Intelligence James Clapper. Contrasting his concerns over the cyber threats presented by China and Russia, Clapper said, "I worry a lot more about the Russians" (Gorman, 2014, para. 2). This study has begun to explain why a person in Clapper's position would say that. We, the United States, as a nation, must react accordingly. To do that, the intelligence community (IC) must refocus on Russia as it has not done since the demise of the Soviet Union in 1991. For example, during the 1970s, U.S. Air Force Intelligence published an English translation of *The Revolution in Military Affairs,* an authoritative publication authored by Soviet military leaders, as part of the Soviet Military Thought Series (Lomov, 1973). After years of focusing on China and the terrorist threat, the IC must once again devote this kind of attention to Russia.

To some extent, the Russians publish their views on some pertinent matters. For example, the current Russian military doctrine mentioned that Russia might use IW, of which cyber-warfare is a subset, to substitute for kinetic weapons (Russian Federation, 2010). The doctrine is

available, however, only in Russian. This indicates the minimum effort that the U.S. IC must make to obtain, translate and distribute relevant documents. However, an appropriate national response to the findings of this study must go beyond translation and language skills in two ways.

First, as this study has shown, an understanding of the Russian language is insufficient to grasp the essence of the Russian cyber threat. What Smith (2014a) called the unique Russian nexus of government, business and crime is unique because it is a product of Russian culture. Consequently, it is important to teach analysts to think in the Russian way. In this regard, the IC could benefit from some of the teachings of Sherman Kent, who some call the father of U.S. intelligence analysis. Kent believed in rigorous training and methodology for intelligence analysts, however, he also recognized that there would always be shortcomings inside the intelligence bureaucracy. Consequently, he advocated use of an extensive network of outside experts (Davis, n.d.).

Second, the kind of analysis featured in this study must be disseminated beyond the IC. Different from the Cold War period, in our globalized era, a variety of government officials, business people and others will have contact with Russians. For example, FBI agents dealing with Russian law enforcement authorities must have a deep understanding of how the Russian polity functions so that they do not assume that their FSB interlocutors share similar values and objectives. Large private organizations—banks, energy companies, online services, etc.—should similarly seek expert advice to inform their dealings with Russia. Such companies invest billions of dollars in projects that could affect the economic and even national security of the U.S.

On the strategic level, the 2007 civil disturbances in Estonia, the 2008 attack on Georgia and the 2013-2014 Russia-Ukraine conflict all indicate that IW will play some role in all future

conflicts to which Russia is a party. As this study has found, Russia sees cyber as a subset of IW, one tool among many, to be selected and used, as appropriate (Heickerö, 2010; Thomas, 1996, 1996-1997). Consequently, the U.S. must assume that IW will be, and cyber-warfare may be, part of any conflict to which Russia is party. Moreover, we should assume that other nation-states, and even some sub-national and trans-national actors, have carefully watched developments in the former Soviet Union and that they have woven cyber techniques into concepts of unrestricted warfare as described by Qiao and Wang (2002). In sum, we should assume that various forms of cyber warfare will be combined with other aggressive measures in war or other hostilities against the U.S., its allies and friends. This requires the U.S. national security community to develop models of such warfare and doctrine to counter it.

In this regard, the U.S. must carefully consider the vulnerabilities of the many relatively weaker allies and friends on which it depends. The 2008 attack on Georgia provided an illustration of this point. Georgia is the gateway to a vital transit corridor between the Black Sea and the Caspian Sea (Smith, 2014c). This corridor is important to U.S. security interests, however, Georgia cannot defend it alone. Consequently, the U.S. must consider Georgia's vulnerability, including its cyber vulnerability, as part of its own security calculations. The US-CCU suggested an international cyber advisory service that could warn and advise a country like Georgia about cyber-attacks (US-CCU, 2009). One need not accept the form in which they present it to take the point that it would be in the interest of the U.S. to coordinate some kind of cyber warning and advisory service for select allies and friends.

A similar point could be made with regard to Russian cyber-espionage, which this study has established is a threat to some countries of the former Soviet Union and the Warsaw Pact and to the U.S. The U.S. national security community must learn more about Russian cyber-

espionage and its criminal connections, however, this leads to another limitation of this study. Some aspects of this study are, in essence, open source intelligence collection and analysis. The required information cannot be gathered in a laboratory experiment or sample survey. It is carefully guarded by criminals and the Russian state. Therefore, it must be prized away and pieced together. Nonetheless, there are two urgent research requirements for the U.S. IC and other security researchers. This study has established that cyber criminals have freedom to operate in Russia, so long as they do not damage the interests of the *siloviki* or the interests of Russia, as the *siloviki* perceive them. Moreover, this study has shown that there is collusion between Russian cyber criminals and the Russian state on cyber-espionage. The study even provided the example of Gyges, in which there appears to have been cross-fertilization of criminal and government malware (Symantec, 2014). The first question for further research, then, is whether cyber-crimes are being committed for geopolitical purposes. For example, are attacks on U.S. financial institutions conducted for purely criminal purposes, or is there some element of political retribution or warning involved? A related set of questions emerges from the example of the Energetic Bear, or Dragonfly APT (Osborne, 2014). Are Russian cyber criminals leaving backdoors in the computer systems of American critical infrastructure? If yes, is there a Russian geopolitical purpose to this activity? The implications of a positive answer would be that Russia is moving beyond espionage against the U.S. to preparation of the battlefield for a possible computer network attack. Finally, to what extent has American critical infrastructure been infected?

The matter of criminal activity on behalf of the geopolitical interests of the Russian state leads back to systemic corruption and a final set of questions for further research. If Russia is a threat to the U.S. and its allies and friends, and if Russia is characterized by systemic corruption,

we need to know more about that corrupt system. Most of the research conducted by academics such as Byrne (2009) focused on the economic and social consequences of systemic corruption. This is understandable because donor organizations like the E.U., for which she now works, are concerned about the efficacy of the aid that they provide. However, as this study has shown, systemic corruption in a large country like Russia can also have national security implications for other countries. Consequently, there should be more research conducted on the effects of systemic corruption on a country's intelligence activities, national security and strategic industries.

With specific regard to Russia, more research is necessary to determine who the individual players are in the unique Russian nexus of government business and crime (Smith, 2014a). Which cyber criminals and which of the *siloviki* matter on geopolitical operations? This study has found that someone involved in contemporary cyber espionage activities appears to be sitting at the same computers that were used in the 2008 attacks on Georgia. If RBN has dissolved, what or who has taken its place?

Finally, researchers, particularly the U.S. IC, should maintain a close watch for development of cyber structures within the Russian military. As this study has shown, Russia has used cyber-warfare in connection with kinetic warfare (US-CCU, 2009) its military has a doctrine for cyber-warfare (Russian Federation, 2010) and senior Russian officials speak about some kind of a military cyber command (RIA Novosti, 2012). Nonetheless, in the words of Keir Giles, "Calls for 'Information Troops' have not yet given rise to any visible change in tasking or designation of military structures" (Giles, 2011, p. 53). This could be because such structures are kept secret and western observers are yet to discover them, or it could be because such structures do not exist. Either way, it would be important to gather as much information as possible about

the development of cyber warfare capabilities in the Russian military. These are the recommendations for action and further research that emerge from this study. Although much work remains to be done, and this study had some limitations, it has firmly established a number of important facts.

Conclusion

The fundamental problem addressed by this study is that Russian cyber threats are often overlooked by U.S. officials. Consequently, Russian cyber challenges are dealt with inadequately, often treated as singular events, rather than as elements of a syndrome. Many Americans misunderstand Russian cyber threats because they are rooted in a system that altogether differs from the expectations of most westerners—a unique nexus of government, business and crime, which is, in turn, deeply rooted in Russian culture and history. Failure to gain a clearer understanding of Russian cyber threats could be catastrophic. The purpose of this research was to build understanding by examining how certain systemic characteristics of contemporary Russia, including its political economic and social systems, have promoted multiple cyber threats to neighboring countries and to the U.S. The utility of this study is that it may help to inform the American foreign policy public about this important matter.

Contemporary Russia is characterized by systemic corruption presided over by President Vladimir Putin, with the *siloviki* playing a major role in every aspect of the system. The systemic corruption skews normal economic development and concentrates what wealth there is in the hands of a few. Meanwhile, the educational system that Russia inherited from the Soviet Union continues to produce people who excel at math and science. With poor job prospects, some of these people are attracted to crime, particularly cyber-crime. In the environment of systemic corruption run by the *siloviki,* cyber criminals can thrive, so long as they do not harm the

interests of the oligarchy or the interests of Russia, as the *siloviki* perceive those interests. In this context, their skills fit very well into a well-developed doctrine of IW. IW, and more specifically cyber techniques, are used to control information, commit espionage and attack neighbors directly. Consequently, some amount of cyber-criminal time and resources is dedicated to Putin's geopolitical agenda. A major finding of this study is that there is collusion between the Russian state and cyber criminals to the point that the latter conduct cyber operations in support of the country's geopolitical aims.

The immediate impact of this is directed at Russia's immediate neighbors, the countries of the former Soviet Union and the Warsaw Pact, however, it also affects U.S. interests in three ways. First, most of the Russian narrative is anti-American. Therefore, allowing Russia to control information in Eastern Europe and Central Asia runs counter to American interests. Second, the U.S. has formal alliances with many of the countries involved and an informal alliance with Georgia. The U.S. relies upon these countries in a variety of ways. Therefore, the vulnerability of these countries to various forms of cyber warfare is also an American vulnerability. Third, as shown by the relationship of Uroburos/Snake/Turla to Agent.BTZ, Russia's cyber espionage also directly targets the U.S.

Moreover, there is a potential fourth Russian cyber challenge to U.S. interests. This study highlighted that prospect by placing information about the Energetic Bear APT in context. Some investigators believe that Energetic Bear has been placing backdoors in the computer systems of U.S. critical infrastructure. If this were correct, it would imply that Russia has moved beyond cyber-espionage to preparation of the battlefield for computer network attack. As the study has shown, Russia has a record of employing cyber warfare and a doctrine for its use. Failure to become fully aware of this prospect could be catastrophic for the U.S. and its allies.

Consequently, one of the major contributions is the recommendation that this be further investigated.

In sum, this study integrated Russian geopolitics, politics economics and society with the results of research into specific computer network events. When that kind of context is considered, Russian cyber threats can be clearly discerned. We ignore them at our peril.

References

Agreement between the governments of the members of the Shanghai Cooperation Organization in the field of international information security. (2008, December 2). *NPR Assets*. Retrieved October 5, 2014, from http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf

Akhvlediani, Z. (2012, May 29). Cyber attacks on Georgian governmental resources. Lecture conducted from Georgian Data Exchange Agency, Ankara, Turkey. Retrieved October 10, 2014 from http://www.slideshare.net/DataExchangeAgency/cyber-attacks-on-georgian-governmental-resources

Andrews, R. (2012, July 12). Google joins protest against Russia's web blacklist. *Gigaom*. Retrieved October 20, 2014, from https://gigaom.com/2012/07/12/google-joins-protest-against-russias-web-blacklist/

Apps, P., & Finkle, J. (2014, March 7). Suspected Russian spyware Turla targets Europe, United States. Retrieved November 1, 2014 from http://www.reuters.com/article/2014/03/07/us-russia-cyberespionage-insight-idUSBREA260YI20140307

Becker, J., & Myers, S. (2014, November 1). Putin's Friend Profits in Purge of Schoolbooks. Retrieved November 2, 2014 from http://www.nytimes.com/2014/11/02/world/europe/putins-friend-profits-in-purge-of-schoolbooks.html?module=Search&mabReward=relbias%3Aw%2C%7B%221%22%3A%22RI%3A7%22%7D&_r=0

Bender, J., & Kelley, M. (2014, March 6). The Ukraine-Russia Cyber War Is Heating Up. *Business Insider*. Retrieved October 16, 2014, from http://www.businessinsider.com/the-ukraine-russia-cyber-war-is-heating-up-2014-3

Byrne, E. (2009, July 31). Definitions and Types of Corruption: Elaine Byrne; academic, journalist, consultant. *Elaine Byrne*. Retrieved October 8, 2014, from http://elaine.ie/2009/07/31/definitions-and-types-of-corruption/

Barrett, D. (2012, March 28). U.S. Outgunned in Hacker War. *The Wall Street Journal*. Retrieved September 27, 2014, from http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html

Brewster, T. (2014, March 19). Criminal Malware Used In Attacks On Ukraine Government. *TechWeekEurope UK*. Retrieved March 26, 2014, from http://www.techweekeurope.co.uk/news/dirtjumper-malware-ukraine-russia-141954

Carman, D. (2002, March). Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass Media and the Politics of Identity . *digital.law*. Retrieved September 27, 2014, from https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/757/16_11PacRimL%26PolyJ339%282002%29.pdf?sequence=1

Carr, J. (2009, June 29). Digital Dao. *: 7 Reasons Why China Isn't The World's Biggest Cyber Threat (And Who Is)*. Retrieved October 30, 2014, from http://jeffreycarr.blogspot.com/2011/06/7-reasons-why-china-isnt-worlds-biggest.html

Carr, J. (2010). *Inside cyber warfare*. Sebastopol, Calif.: O'Reilly Media, Inc.

Chernenko, E., & Safronov, I. (2012, October 18). NATO vybralo uslovnogo kiberprotivnika. [NATO chooses provisional cyber enemy] *Kommersant*. Retrieved October 13, 2014, from http://www.kommersant.ru/doc/2046919

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: the next threat to national security and what to do about it*. New York: Ecco.

Clover, C. (2009, March 11). Kremlin-backed group behind Estonia cyber blitz - FT.com. *Financial Times*. Retrieved December 1, 2010, from http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html?siteedition=intl#axzz3GRnmyEoc

Convention on Cybercrime. (n.d.). *Council of Europe*. Retrieved October 13, 2014, from http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

Corbin, K. (2009, March 12). Lessons From the Russia-Georgia Cyberwar. *InternetNews.com*. Retrieved September 27, 2014, from http://www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm

Cyber Warfare: Beyond Estonia-Russia. (2007, May 30). *mi2g*. Retrieved September 27, 2014, from http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/media.php

Davis, J. (n.d.). Sherman Kent and the Profession of Intelligence Analysis. *CIA: The Sherman Kent Center for Intelligence Analysis*. Retrieved June 17, 2014, from https://www.cia.gov/library/kent-center-occasional-papers/pdf/OPNo5.pdf

Egan, M. (2010, November 19). Cyber Spies Pose Looming Threat. *Fox Business*. Retrieved September 27, 2014, from http://www.foxbusiness.com/markets/2010/11/19/businesses-risk-cyber-espionage/

Emerging Threat: Dragonfly / Energetic Bear – APT Group. (2014, August 8).*Symantec*. Retrieved September 27, 2014, from http://www.symantec.com/connect/blogs/emerging-threat-dragonfly-energetic-bear-apt-group

Felshtinsky, Y., & Litvinenko, A. (2007). *Blowing up Russia: the secret plot to bring back KGB terror: acts of terror, abductions, and contract killings organized by the Federal Security Service of the Russian Federation*. New York: Encounter Books.

Felshtinsky, Y., & Pribylovsky, V. (2008). *The corporation: Russia and the KGB in the age of President Putin*. New York: Encounter Books.

Finn, P. (2007, April 28). Statue's Removal Sparks Violent Protests in Estonia. *Washington Post*. Retrieved October 18, 2014, from http://www.washingtonpost.com/wp-dyn/content/article/2007/04/27/AR2007042702434.html

Flook, K. (2009, May 13). AEI Critical Threats. *Russia and the Cyber Threat*. Retrieved October 13, 2014, from http://www.criticalthreats.org/russia/russia-and-cyber-threat#_ftnref13

Foreign Spies Stealing U.S. Economic Secrets in Cyberspace. (2011, October). *ncix.gov*. Retrieved September 27, 2014, from http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Giles, G. (2011, January 1). "Information Troops" - A Russian cyber command? *Conflict Studies Research Centre*. Retrieved November 20, 2012, from http://www.conflictstudies.org.uk/files/Russian_Cyber_Command.pdf

Giles, K. (2014, March 11). With Russia and Ukraine, is all really quiet on the cyber front?. *Ars Technica*. Retrieved March 13, 2014, from http://arstechnica.com/tech-policy/2014/03/with-russia-and-ukraine-is-all-really-quiet-on-the-cyber-front/

Gjelten, T. (2010, September 23). Seeing the Internet as an 'Information Weapon'. *NPR*. Retrieved October 13, 2014, from http://www.npr.org/templates/story/story.php?storyId=130052701

Goncharov, M. (2012). Russian Underground 101. *Trend Micro*. Retrieved October 5, 2014, from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Gorman, S. (2009, April 8). Electricity Grid in U.S. Penetrated By Spies. *The Wall Street Journal*. Retrieved September 27, 2014, from http://online.wsj.com/article/SB123914805204099085.html

Gorman, S. (2014, October 17). Intel Chief: Russia Tops China as Cyber Threat.*Washington Wire RSS*. Retrieved October 30, 2014, from http://blogs.wsj.com/washwire/2014/10/17/intel-chief-russia-tops-china-as-cyber-threat/

Government of Georgia, Ministry of Foreign Affairs. Russian Cyberwar on Georgia. (2008, November 10). Retrieved October 16, 2014, from http://www.mfa.gov.ge/files/556_10535_798405_Annex87_CyberAttacks.pdf

Hare, F. (2010). The Cyber Threat to National Security: Why Can't We Agree?. *CCDCOE*. Retrieved September 27, 2014, from http://www.ccdcoe.org/publications/2010proceedings/Hare%20-%20The%20Cyber%20Threat%20to%20National%20Security%20Why%20Cant%20We%20Agree.pdf

Heickerö, R. (2010, March). FOI - Swedish Defence Research Agency. *Emerging Cyber threats and Russian views on information warfare and information operations*. Retrieved October 5, 1014, from http://www.foi.se/ReportFiles/foir_2970.pdf

How Turla and "worst breach of U.S. military computers in history" are connected. (2014, March 12). Retrieved November 1, 2014 from http://www.kaspersky.com/about/news/virus/2014/How-Turla-and-worst-breach-of-US-military-computers-in-history-are-connected

Kelly, J., & Almann, L. (2008, December 2008-January 2009). eWMDs. *Hoover Institution*. Retrieved

October 7, 2014, from http://www.hoover.org/research/ewmds

Kievit, J., & Metz, S. (1995, June). Strategy and the Revolution in Military Affairs: From Theory to Policy. *Strategic Studies Institute*. Retrieved September 27, 2014, from http://www.strategicstudiesinstitute.army.mil/pubs/summary.cfm?q=236

Lally, K., & Englund, W. (2012, December 6). Russia fumes as U.S. Senate passes measure aimed at human rights. Retrieved November 2, 2014, from http://www.washingtonpost.com/world/europe/us-passes-magnitsky-bill-aimed-at-russia/2012/12/06/262a5bba-3fd5-11e2-bca3-aadc9b7e29c5_story.htmlLee, D. (2014, March 5). Cyber 'stand-off' in Ukraine crisis. *BBC News*. Retrieved October 16, 2014, from http://www.bbc.com/news/technology-26447200

Lomov, N. (Ed.). (1973). *The Revolution in Military Affairs*. Moscow: Ministry of Defense of the USSR (translated and published by the U.S. Air Force).

Lynn, W. (2010, September/October). Defending a New Domain. *Foreign Affairs*. Retrieved September 27, 2014, from http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

Markoff, J. (2008, August 12). Before the Gunfire, Cyberattacks. *The New York Times*. Retrieved October 12, 2014, from http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0

Mshvidobadze, K. (2009). Cyber War, Cyber Defense. *NATO New Strategic Concept, Romanian Approach* (p. 280). Bucharest: Editura Curtea Veche.

Nacionalnaja bezopasnost Rossii: Informacionnaja bezopasnost Rossii. (2012, February 3). *Rossijskaja Federacija, Sovet bezopasnosti*. [National Security of Russia: Information Security of Russia. *Russian Federation, Council of National Security.*] Retrieved October 14, 2014, from http://www.scrf.gov.ru/documents/6/113.html

Nossik, A. (2011, April 1). DDoS v Rossii: istorija voprosa. *Snob.ru*. [DDoS in Russia: history of the question] Retrieved December 31, 2012, from http://www.snob.ru/selected/entry/33684

Organski, A. F. (1968). *World politics,* (2d ed.). New York: Knopf.

Osborne, C. (2014, August 18). Government-grade malware in hacker hands ZDNet. *ZDNet*. Retrieved September 27, 2014, from http://www.zdnet.com/government-grade-malware-in-hacker-hands-7000031765/

Overview by the US-CCU of the cyber campaign against Georgia in August of 2008. (2009, August). *Registan*. Retrieved September 27, 2014, from http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

Pakharenko, G. (2014, March 27). Cyber attacks in the Ukraine Quantitative Analysis December 2013 - March 2014. *Anti-Phishing Working Group*. Lecture conducted from Anti-Phishing Working Group, Kiev, Ukraine.

Peters, S. (2014, July 17). Government-Grade Stealth Malware In Hands Of Criminals. *Dark Reading*. Retrieved October 18, 2014, from http://www.darkreading.com/government-grade-stealth-malware-in-hands-of-criminals/d/d-id/1297362

Politkovskaia, A. (2005). *Putin's Russia: life in a failing democracy*. New York: Metropolitan Books.

Project Grey Goose Phase I Report. (2008, October 17). *Scribd*. Retrieved October 20, 2014, from https://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report

Rahn, C., Khrennikov, I., & Eglitis, A. (2014, March 6). Russia-Ukraine Standoff Going Online as Hackers Attack. *Bloomberg.com*. Retrieved March 7, 2014, from http://www.bloomberg.com/news/2014-03-05/russia-ukraine-standoff-going-online-as-

hackers-attack.html

RIA Novosti. (2012, March 21). Russia Considering Cyber-Security Command. *RIA Novosti*. Retrieved October 14, 2014, from http://en.rian.ru/russia/20120321/172301330.html

Russon, M. (2014, March 4). Ukraine Crisis: Cyber War with Russia Heating up. *International Business Times RSS*. Retrieved March 6, 2014, from http://www.ibtimes.co.uk/ukraine-crisis-cyber-war-russia-heating-1438890

Satter, D. (2003). *Darkness at dawn: the rise of the Russian criminal state*. New Haven: Yale University Press.

Smith, D. (2012, August). How Russia Harnesses Cyberwarfare. *Defense Dossier*. Retrieved October 1, 2014, from http://www.afpc.org/files/august2012.pdf

Smith, D. (2014a, January). Russian Cyber Capabilities, Policy and Practice. *inFocus Quarterly Journal*. Retrieved October 9, 2014, from http://www.jewishpolicycenter.org/4924/russian-cyber-capabilities

Smith, D. (2014b, April 26). Ukraine 2014: Fiber Optics and Geopolitics. Lecture at Utica College, Utica, NY.

Smith, D. (2014c). *Azerbaijan and Georgia: The Enduring Strategic Importance of the South Caucasus East-West Corridor.* Tbilisi, Georgia: Georgian Foundation for Strategic and International Studies.

Smith, D. & Mshvidobadze, K., (2011, May 16). Russia, Georgia and the Shape of Cyber Wars to Come. *Cyber Defence Conference*. Lecture conducted from SMi / Cyber Security Forum Initiative, Istanbul, Turkey. Retrieved October 15, 2014 from http://gfsis.org/media/download/GSAC/cyberwar/Shape_of_Cyber_Wars.pdf

Snake campaign & cyber espionage toolkit. (n.d.). *BAE Systems*. Retrieved October 15, 2014,

from http://info.baesystemsdetica.com/rs/baesystems/images/snake_whitepaper.pdf

Software Development in Ukraine. (2008, November). *Munk, Andersen and Feilberg*. Retrieved October 6, 2014, from http://www.mafcon.com/downloads/ITknowhow.pdf

SORM 3. (n.d.). *14prog.ru*. Retrieved October 20, 2014, from http://14prog.ru/main/sorm3.aspx

Strategija nacional'noj bezopasnosti Rossijskoj Federacii do 2020 goda [National Security Strategy of the Russian Federation to 2020]. (2009, May 12). *Sovet Bezopasnosti Rossijskoj Federacii.* [The Security Council of the Russian Federation]. Retrieved September 27, 2014, from http://www.scrf.gov.ru/documents/1/99.html

Talbot, D. (2010, April 14). Cybercrime needs to be top priority, says Obama aide. *MIT Technology Review*. Retrieved November 20, 2012, from http://m.technologyreview.com/computing/25074/

Thomas, T. (1996-1997, Winter). Foreign Military Studies Office Publications - Deterring Information Warfare: A New Strategic Challenge. *Foreign Military Studies Office Publications - Deterring Information Warfare: A New Strategic Challenge*. Retrieved October 13, 2014, from http://fmso.leavenworth.army.mil/documents/deteriw.htm

Thomas, T. (1996). Russian views on information-based warfare. *Airpower Journal - Special Edition 1996*. Retrieved October 6, 2014, from http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/spec96/thomas.pdf

Thomson, I. (2007, May 31). Russia 'hired botnets' for Estonia cyber-war. *V3.co.uk*. Retrieved October 18, 2014, from http://www.v3.co.uk/v3-uk/news/1974750/russia-hired-botnets-estonia-cyber-war

Torbakov, I. (2003, October 26). Russian Policymakers Air Notion of "Liberal Empire" in Caucasus, Central Asia. *EurasiaNet.org*. Retrieved September 27, 2014, from

http://www.eurasianet.org/departments/insight/articles/eav102703.shtml

Ukaz Prezidenta Rossijskoj Federacii ot 15 janvarja 2013 g. N 31s. Moscow [Order of the President of the Russian Federation of 15 January 2013 g. N 31s]. (2013, January 18). *Rossijskaja Gazeta.* Retrieved September 27, 2014, from http://www.rg.ru/2013/01/18/komp-ataki-site-dok.html

Uroburos: Highly complex espionage software with Russian roots. (2014, January 1). *GData Software*. Retrieved October 15, 2014, from https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf

Voennaja doktrina Rossijskoj Federacii [Military Doctrine of The Russian Federation]. (2010, February 5). *Prezident Rossii* [President of Russia]. Retrieved September 27, 2014, from http://news.kremlin.ru/ref_notes/461

Vserossijskij konkurs nauchno-issledovatel'skih rabot sredi grazhdan Rossijskoj Federacii v interesah Vooruzhennyh Sil Rossijskoj Federacii. (2012, October 10). *Ministerstvo oborony Rossijskoj Federacii*. [All-Russian competition for scientific research among the citizens of the Russian Federation for the armed forces of the Russian Federation, *Ministry of Defense of Russian Federation*] Retrieved November 20, 2012, from http://ens.mil.ru/education/contests/more.htm?id=1719@morfSimpleEvent