All material compiled from open-source documents.

RUSSIA'S IMPLEMENTATION OF HYBRID WARFARE: ESTONIA ('07), GEORGIA ('08), CRIMEA ('14)

Michael C. Mastalski
Capt, United States Air Force

Submitted in fulfillment of the requirements for

AIR UNIVERSITY ADVANCED RESEARCH (NEXT GENERATION INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE)

in part of

SQUADRON OFFICER SCHOOL
VIRTUAL – IN RESIDENCE
AIR UNIVERSITY
MAXWELL AIR FORCE BASE
February 2021

Advisor: Col Darin M. Gregg
Vice Commander/LeMay Center for Doctrine Development and Education
Maxwell AFB, AL

THIS PAGE HAS INTENTIONALLY BEEN LEFT BLANK

Abstract

Russia, through the years, has been perfecting and implementing Hybrid Warfare on their adversaries. This paper will identify commonalities between Russia's engagements with Estonia, Georgia, and Crimea. Russia's hybrid warfare strategies are broken down into three characteristics; economize the use of force, persistence, population-centric. And three typical objectives; capture territory without conventional forces, create a pretext for conventional military action, and hybrid measures to influence politics and policies. Estonia, Georgia, and Crimea all experienced Russia's hybrid mix of cyber and information warfare, while Georgia and Crimea saw it escalate to conventional military action. These actions are persistent with gaining experience to apply methods on Western governments, specifically the U.S.

THIS PAGE HAS INTENTIONALLY BEEN LEFT BLANK

Hybrid Warfare: Russian Implementation

Hybrid warfare – also partially known as grey zone conflict or low-intensity conflict - is a reality, and the United States (U.S.) military must be ready to confront and deter it from peer-to-peer adversaries.[1] The U.S. defines grey zone conflict as actions that seek to gain an advantage without provoking a conventional military response[2]. Still, Russia's definition of hybrid warfare takes it beyond the grey zone depending on their desired outcome. As used today in reference to Russia, "hybrid warfare" refers to Moscow's use of a broad range of subversive instruments, many of which are nonmilitary, to further Russian national interests.[3] Russia has adapted their idea of hybrid warfare as a way to divide and weaken NATO allies; deter or subvert pro-western influence; create pretexts for war; annex territory; to ensure access to European markets on its own terms.[4]

This paper addresses the key characteristics of the Russian hybrid warfare strategy. The three characteristics are to economize the use of force, persistence, continuous attacks, and population-centric.[5] Russia's continuous objectives, specifically during attacks on Estonia ('07), Georgia ('08), and Crimea ('14), was to capture territory without conventional military force if possible, create a pretext for conventional military action if needed, and hybrid measures to influence politics and policies on targets and pro-Western states.[6] All three incidents will be

[1] Jim Garamone, "Military Must Be Ready to Confront Hybrid Threats, Intel Official Says," U.S. DEPARTMENT OF DEFENSE, September 4, 2019, https://www.defense.gov/Explore/News/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intelligence-official-says/.
[2] Ronald J Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War," Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia war, February 2012, https://www.jstor.org/stable/26301960?seq=1.
[3] Christopher S Chivvis, "Understanding Russian 'Hybrid Warfare' and What Can Be Done About It," March 22, 2017, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.
[4] ibid
[5] ibid
[6] ibid

broke down within the three key characteristics, addressing the similarities between them and the perfected escalation from Estonia to Crimea. Following the characteristics, it will address experts educated opinions on Russia's desired objectives. Finally, the paper will briefly cover what the U.S. and allies can do to potentially limit Russia's effectiveness of attacks on U.S. and European Union (EU) infostructures.

Hybrid Characteristics & Objectives of Hybrid Warfare

Estonia in 2007 saw first-hand Russia's hybrid warfare capabilities when attacked with extreme and effective information and cyber ops. Once separated after the cold war, Estonia became a marvel of e-government, where online procedure was dominant. Estonia had managed to build a new infostructure for the citizens and government to operate into the future. On 27 April 2007, a cyber-attack on their government ministries, political organizations, newspapers, banks, and companies' websites commenced.[7] In computer language, Estonia had seen a wave of Distributed Denial of Service attacks (DDoS) and Botnets (computers hacked from remote sites and controlled to unwittingly deliver spam and viruses to any location in the globe).[8]

Many of these attacks traced back to servers in Egypt, Russia, and The U.S.[9] Internet chatter on forums was heavy with instructions on how to overwhelm Estonian websites with traffic.[10] What makes these types of attacks significant is that Botnet attacks involve millions of computers worldwide controlled by a sole operator, increasing the number of attacks tenfold. Government and Bank websites typically received 1,000 visits a day, but during the attack were

[7] Binoy Kampmark, "Cyber Warfare Between Estonia and Russia," *Contemporary Review* 289 (2007): pp. 288-293.
[8] ibid
[9] Stephen Herzong, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinatiional Responses," *Journal of Strategic Security* 4, no. 2 (2011): pp. 49-60, https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss.
[10] ibid

hit with 2,000 hits a second.[11]These attacks overwhelmed their websites, causing them to crash, preventing the use of them through any means. During these, Russia's primary objectives were to ensure the Estonia government could not communicate with the country or other governments about what was going on.

Additionally, these attacks defaced government sites while pushing Russian propaganda and graffiti to label Estonia party leaders as Nazi's, affecting the populous perception. Simultaneously, the Estonian banks' cyber-attacks required them to report losses estimated at around $1 million. The actions of these attacks prevented credit card and automatic teller machine transactions from occurring for several days.[12] Cyber-attacks maintained the characteristic of persistence, where attacks continued for days, intensifying with each passing day. Russia's attacks were significant at impacting the phycological effects on the Estonian populace and the disruption and loss of trust between citizens and the government.

These types of attacks were significant due to the exploitation of a vulnerable system perceived to be untouchable. Russia's cyber-attacks on Estonia proved that "cyber terrorism" is capable of shutting down critical national infrastructures (such as energy, transportation, and government operations) in an attempt to coerce or intimidate a government or civilian population.[13]

Georgia, in August of 2008, saw almost the same cyber and informational attacks on all the same websites and infostructures. The first phase of these attacks commenced on the evening

[11] ibid
[12] ibid
[13] ibid

of 7 August when hackers launched the same form of DDoS attacks that Estonia experienced.[14] According to Arbor Networks' analysis, the observed DDoS traffic average duration of each surge was two hours and fifteen minutes – the longest lasted six hours.[15] Again, the cyber-attacks targeted the crippling of the countries' government's ability to communicate events as they happened while attempting to correct Russian propaganda. These events had such debilitating consequences for essential services, the National Bank of Georgia ordered all banks to stop offering electronic services. Bank services didn't fully resume until 18 August.

Cyber activity in Georgia shifted to the recruitment of "patriotic" Russian "hacktivists."[16] Much of the recruitment happened through various sites, the most infamous of which was StopGeorgia.ru.[17] Some believe that there were indicators of preparation well before these August attacks; July 2008 when servers were flooded with "win+love+in+Russia," while analysis of graffiti images discovered the images created as early as 2006.[18]

The second phase of these attacks was in sync with the ground operations of Russian forces into Georgia. Many experts claim that the cyber-attacks and propaganda assisted the pretext of conventional force's entry into Georgia. Signs of escalation were evident, which played well into Russia's hybrid strategy. Because relations between the parties had been deteriorating for a while, Russia and Georgia seemed to take preemptive measures in case of an escalation of aggression. Russia at the time was conducting military exercises at several points of the border.

---

[14] Paulo Shakarian and Andrew Ruef, "Chapter 3: How Cyber Attacks Augmented Russian Military Operations," in *Introducation to Cyber-Warfare: A Multidisciplinary Approach*, ed. Jana Shakarian (Burlington, MA: Syngress, 2013), pp. 24-28.
[15] Deibert, Ronald J, Rafal Rohozinski, and Masashi Crete-Nishihata. Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia war, February 2012. https://www.jstor.org/stable/26301960?seq=1
[16] ibid
[17] ibid
[18] ibid

Between July and August 2008, Russia had 8000 soldiers and heavy military hardware in the area that remained on high alert.[19] On the evening of 7 August 2008, the Georgian military entered the South Ossetian capital and several other villages because they claimed that they were responding to South Ossetian soldiers' bombardments that ignored a previously established cease-fire.[20] On 8 August 2008, Russia responded to the Georgian invasion of South Ossetia with superior military force because they saw Georgian actions as a threat.[21] This was the first time Moscow deployed its military forces outside of its borders since the war in Afghanistan in 1979.[22]

Crimea attacks were slightly different from the Estonia and Georgia attacks. However, the beginning stages of cyber-attacks through DDoS and Botnets were identical in producing their desired outcome. But these attacks intensified due to exchanging cyber attacks between both countries due to the revolution in Keiv.[23] Tensions rose due to the 2014 Ukrainian revolution, in which the government of President Viktor Yanukovych was ousted after a popular revolt.[24] Contrary to the protests, the region had groups that desired the integration of Crimea and Russia. 1 March 2014, the de facto Crimean Prime Minister Sergey Aksyonov appealed directly to Russian President Vladimir Putin in a signed statement calling for Russia to "assist in ensuring

[19] The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict, May 24, 2012. https://www.afcea.org/committees/cyber/documents/therusso-georgianwar2008.pdf
[20] ibid
[21] ibid
[22] ibid
[23] Pierluigi Paganini, "Crimea – The Russian Cyber Strategy to Hit Ukraine," Crimea - The Russian Cyber Strategy to Hit Ukraine (Infosec Resources, March 11, 2014), https://resources.infosecinstitute.com/topic/crimea-russian-cyber-strategy-hit-ukraine/.
[24] ibid

peace and tranquility on the territory of Crimea."[25] After these events occurred, the Russian parliament approved President Vladimir Putin's orders to use military force in Ukraine.

Because of this approval, state-sponsored cyber units, groups of hacktivists, and cybercriminals started their intensified campaigns against enemies.[26] Instead of conventional forces, Russia sent in pro-Russian armed soldiers without insignia known as the "green men." In addition to the cyber-attacks already in place, these soldiers had seized buildings and Crimea assets. The attackers also used specialized equipment installed within Ukrtelecom networks in the Crimea region.[27] The installed devices degraded Ukraine's mobile phone infrastructure that targeted parliament members.[28]

Ultimately these attacks, like Estonia and Georgia, prevented the government from communicating with the world and its citizens, allowing Russia to control the chain of events. The green men also set up roadblocks to isolate Crimea from the rest of Ukraine. Concurrently, the Russian military maneuvered their naval vessels in the port of Sevastopol that security experts believed was a mission to isolate the region. Many units were carrying jamming equipment to block radio communications. Along with the cyberattacks, this denial act isolated Crimea to the point they relied on foreign governments, including Russia, for nearly 70% of its internet exchange capacity.[29] These moves ultimately affected the political and economic influence on the region.

---

[25] "Ukraine Crisis: Crimea Leader Appeals to Putin for Help," BBC News (BBC, March 1, 2014), https://www.bbc.com/news/world-europe-26397323.
[26] ibid
[27] ibid
[28] Roger McDermott, "Russia's Information Campaign in Crimea: Nodes, Themes and Caution," Russia's Information Campaign in Crimea: Nodes, Themes and Caution, September 20, 2016, https://jamestown.org/program/russias-information-campaign-in-crimea-nodes-themes-and-caution/.
[29] ibid

Strategies to Counter Hybrid Warfare

Countering the challenges posed by the Russian government and their implementation of hybrid warfare will take time, effort, and resources. Practical strategies to defend the U.S., NATO and the EU against Russian hybrid strategy will include, at a minimum, the following.

Analyze the Kremlin's decisions within the Russian framework of hybrid war to understand and mitigate Russian lines of effort. Obfuscating the nature and purpose of Kremlin activities is a crucial objective of hybrid warfare, and U.S. confusion about the term and the Russian approach to such conflicts hinders the development of effective counterstrategies.[30]

Increase collaboration between U.S. agencies, NATO, and EU.

Because hybrid warfare can affect the U.S. State Department, the Defense Department, the Treasury Department, the intelligence community, and NATO's equivalent, combining doctrine is essential. Since 2015, NATO has had a strategy to counter hybrid warfare and ensures that the Alliance and Allies are sufficiently prepared. And that they will deter hybrid attacks on the Alliance, if necessary, will defend Allies.[31]

Develop appropriate resource allocation to the collection and analysis of intelligence in the European theater.

The U.S., NATO, and EU members must ensure that they have the necessary resources to meet the growing threats. Each must be more transparent with each other to provide a solid collected amount of intelligence. Intelligence is vital to tracking and advanced warning of

[30] Mason Clark, "Russian Hybrid Warfare," September 2020, http://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf.
[31] Nato. "NATO's Response to Hybrid Threats." NATO, May 28, 2019. https://www.nato.int/cps/en/natohq/topics_156338.htm.

Russian hybrid activities. To successfully combat these issues, individual intelligence agencies from all partners much be closely linked.

Support transparency and anti-corruption efforts abroad and at home.

Tolerance of corruption greatly facilitates Russian influence strategies.[32] The U.S. must support European anti-corruption efforts, with appropriate funding for related State Department and U.S. Agency for International Development programs.[33]

Russia has continually proven it can implement its hybrid warfare to help push its agenda. Though not definitively proven that Russia has tampered with or influenced recent U.S. elections, it certainly carries that type of stigma. Nevertheless, Russia's threat and growing challenge are undoubtedly real, with no chance of going away any time soon. The U.S., NATO, and EU must continue to recognize the threat and continue moving forward together to counter.

[32] ibid
[33] ibid

Bibliography

Chabrow, Eric, and Ron Ross. Cyber's Role in Ukraine-Russia Conflict, 4 March, 2014. https://www.bankinfosecurity.com/cybers-role-in-ukraine-russia-conflict-a-6597.

Chivvis, Christopher S. "Understanding Russian' Hybrid Warfare' and What Can Be Done About It," 22 March, 2017. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf.

Clark, Mason. "Russian Hybrid Warfare," September 2020. http://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf.

"Competing in the Gray Zone." Competing in the Gray Zone | Center for Strategic and International Studies, 7 December, 2018. http://www.csis.org/features/competing-gray-zone.

Deibert, Ronald J, Rafal Rohozinski, and Masashi Crete-Nishihata. Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia war, February 2012. https://www.jstor.org/stable/26301960?seq=1.

Garamone, Jim. "Military Must Be Ready to Confront Hybrid Threats, Intel Official Says." U.S. DEPARTMENT OF DEFENSE, 4 September, 2019. https://www.defense.gov/Explore/News/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intelligence-official-says/.

"Georgia Was Going to Capture Abkhazia 9,000 Soldiers." Lenta.Ru, 27 August, 2008. https://lenta.ru/news/2008/08/27/nogovitsyn2/.

Herzong, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49–60. https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss.

Kampmark, Binoy. "Cyber Warfare Between Estonia and Russia." *Contemporary Review* 289 (2007): 288–93.

McDermott, Roger. Russia's Information Campaign in Crimea: Nodes, Themes and Caution, 20 September, 2016. https://jamestown.org/program/russias-information-campaign-in-crimea-nodes-themes-and-caution/.

Miniats, Madelena Anna. War Nerves: Russia's Use of Cyber Warfare in Estonia, Georgia, and Ukraine, May 2019. https://digitalcommons.bard.edu/cgi/viewcontent.cgi?article=1191&context=senproj_s2019.

Nato. “NATO's Response to Hybrid Threats." NATO, 28 May, 2019. https://www.nato.int/cps/en/natohq/topics_156338.htm.

Paganini, Pierluigi. "Crimea – The Russian Cyber Strategy to Hit Ukraine." Crimea - The Russian Cyber Strategy to Hit Ukraine. Infosec Resources, 11 March, 2014. https://resources.infosecinstitute.com/topic/crimea-russian-cyber-strategy-hit-ukraine/.

The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict, 24 May, 2012. https://www.afcea.org/committees/cyber/documents/therusso-georgianwar2008.pdf.

Shakarian, Paulo, and Andrew Ruef. "Chapter 3: How Cyber Attacks Augmented Russian Military Operations." Essay. In *Introduction to Cyber-Warfare: A Multidisciplinary Approach*, edited by Jana Shakarian, 24–28. Burlington, MA: Syngress, 2013.

"Ukraine Crisis: Crimea Leader Appeals to Putin for Help." BBC News. BBC, 1 March, 2014. https://www.bbc.com/news/world-europe-26397323.