War of Nerves: Russia's Use of Cyber Warfare in Estonia, Georgia and Ukraine

Madelena Anna Miniats
Bard Colllege

War of Nerves:

Russia's Use of Cyber Warfare
in Estonia, Georgia and Ukraine

Senior Project Submitted to
The Division of Global and International Studies
of Bard College

By
Madelena Miniats

Annandale-on-Hudson, NY
May 2019

Abstract

This project examines how Soviet military thought has influenced present day Russian military doctrine and has evolved to include cyber warfare as part of the larger structure of Russian information warfare. The analysis of three case studies of Russian cyber activity, the attack on Estonia (2007), the Russian-Georgian war (2008) and the ongoing Ukrainian war (beginning 2014), demonstrates the continuity of military doctrine and the physical manifestation of Russia's cyber capabilities.

Acknowledgements

First and foremost I would like to acknowledge the fact that the title of this thesis is named “War of Nerves,” as this experience has been a “war of nerves,” with that being said:

To my mom, thank you for always guiding, giving me strength, love and support when I needed it most; tirelessly teaching me to edit my work since I first learned how to write. I would not be the woman I am today without your unconditional love - Es tevi mīlu.

To my grandparents, for always believing in me in everything that I do, and in every adventure I set my mind to - Bučas.

To my dad and Martye, thank you for the late night pep talks, words of support and the endless belly laughs. You are my rocks when everything else seems to come apart - Aš myliu jus abu.

To my colleagues at the American Latvian Youth Association, thank you all for stepping up when I needed it the most, it means the world to me to know that I have a support system like you in my life - Paldies.

To my friends, thank you for always bringing a smile to my face and lifting me. No amount of Venti Strawberry Açaís will ever express how much I've appreciated you guys throughout this process.

And last but not least - thank you to my advisor Jonathan Becker for guiding me through these two semesters and finding the time to meet with me amid the bustle. I appreciate the knowledge and discipline you have instilled in me and in my writing.

Table of Contents

Introduction

The famous military strategist and thinker Carl von Clausewitz once stated that "usually before we have learnt what danger really is, we form an idea of it which is rather more attractive than repulsive."[1] Back in 2012, the world community began flirting with cyber, viewing it as a new form of conducting warfare between states. In 2012, the United States, in collaboration with Israel, was responsible for the infamous Stuxnet attack, or "Operation Olympic Games," on Iran's Natanz uranium enrichment facility. Dubbed as "Year One"[2] by cyber expert and author Adam Segal, the year 2012 is now perceived as the starting point of international engagement in the realm of cyberspace. This classified attack, implemented with great precision and intensive planning, was designed to cause damage to the enrichment facility, as well as to disrupt the development of Iran's nuclear program. The physical consequences of the attack were massive, as more than 1,000 Iranian centrifuges were damaged.[3] In addition, the malware, or malicious software,[4] used in the attack spread to more than a hundred countries across the world. Although cyber had been employed by states on a subdued level since the 1990s,[5] no one can deny that this was the first time such a massive attack was administered by a country in which physical damage was caused to an adversary's infrastructure.

Five years earlier, in 2007, tensions had risen between the ethnic Russian population of Estonia protesting the removal of the Soviet Bronze Soldier statue from its prominent location in

[1] Dexter, "Clausewitz and Soviet Strategy," 50.
[2] Segal, *The Hacked World Order*, 2.
[3] Ibid.
[4] "Malicious software is any software that gives partial to full control of your computer to do whatever the malware creator wants. Malware can be a virus, worm, trojan, adware, spyware, root kit, etc. The damage done can vary from something slight as changing the author's name on a document to full control of your machine without your ability to easily find out. Most malware requires the user to initiate it's operation. Some vectors of attack include attachments in e-mails, browsing a malicious website that installs software after the user clicks ok on a pop-up, and from vulnerabilities in the operating system or programs." "Malicious Software."
[5] Segal, 1.

the capital city of Tallinn, after the newly elected conservative Estonian government called for the removal of the statue. The ethnic Russian population voiced concerns over the removal, to which the Kremlin responded condemning the Estonian government for infringing upon the rights of the local ethnic Russian population. The “Bronze Night” protests took place between April 26th to April 29th in 2007 as response to the statue’s removal, erupting in riots. The botnets (or previously hacked computers that have the ability to send out information, overwhelming an internet server) aided in administering and carrying out the DDoS, or distributed denial-of-service attack. As a result, a series of DDoS attacks targeted multiple government websites, including those of the Estonian parliament, the defense minister, and major universities and national newspapers. As one of the most connected and technologically advanced countries in the world, Estonia in 2007, relied almost entirely on the internet for daily communication and functioning of the state. Estonia became paralyzed for an extended period of time, even after the initial attack. This was the first time a state used offensive tactics in the cyber realm to change the actions of another country. Instead of the Stuxnet operation, it is the attack on Estonia in 2007 which should be regarded as “Year One.” This attack set the precedent that if it was successful in Estonia, the most technologically advanced country in the world -- it could be successful anywhere.

Scholars and experts alike have had to familiarize themselves with cyber as a new way of *understanding* war in the twentieth century, including direct cyber attacks such as Stuxnet, but not necessarily defining it as an entirely new form of warfare. Mark Galeotti, from the Center for Global Affairs at New York University, argues that cyber warfare is not necessarily a new form of warfare when contextualized in relation to the broader world where the political, military, social and technological spheres are all constantly in flux.[6] Michael Connell and Sarah Vogler emphasize that cyber cannot fit into a "one-size-fits-all definition," highlighting that since cyber can be implemented in a variety of ways, it also adds to the complexity of the issues treated in the literature on cyber. Maness and Valeriano suggest that instead of conceptualizing cyber as a separate form of warfare, it should be thought of as a tactic used in furthering foreign policy.[7] James Wirtz writes that the cyber realm often feels disconnected from the larger geopolitical framework due to the stigma that enshrouds cyber, especially following high profile cyber attacks such as Stuxnet. Although a basic knowledge of the issues surrounding cyber is necessary, for the purposes of this paper the specific literature on Russia's use of cyber is more crucial.

The literature on Russia's use of cyber generally agrees that Russia's goal is to be able to defeat the enemy without having to fire a shot. The Russian government uses information and cyber warfare as a way of "preparing the battlespace,"[8] with the intent to have total control of the information space, which becomes critical in times of conflict. Such a system of information control allows for the state to be consistently prepared in times of peace and war alike. Jānis Bērziņš, of the National Defense Academy of Latvia, asserts that in analyzing Russia's use of cyber it is to noteworthy that the most important battlespace, in the Kremlin's point of view, is of that of the mind. In the future, information and psychological warfare are to take precedence in "depressing" the enemy from within, thereby minimizing the need for deploying hard military power.[9] Connell and Vogler also emphasize that it is important to understand Russian cyber as an

[6] Galeotti, "Hybrid, Ambiguous, and Non-Linear?," 297.
[7] Maness and Valeriano, "The Impact of Cyber Conflict on International Interactions," 303.
[8] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," 5.
[9] Bērziņš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy," 3.

element in their broader use of information warfare, which means that the state is not only able to "justify its actions in the eyes of the public,"[10] but as Wirtz also points out, to be able to dominate the information landscape in any conflict and be able to control the discourse on both sides.[11] Nikolas Gvosdev, author of *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, states that what Russia excels at is the ability to implement characteristically unsophisticated cyber attacks in a sophisticated fashion.[12]

In view of the existing literature considering Russia's use of cyber warfare to be a part of its larger infrastructure of information warfare, in this paper I will attempt to answer the question: Is Russia's use of cyber warfare a new form of warfare, or is it an extension of past Soviet doctrine? Specifically, can we trace Russian cyber warfare to Soviet asymmetric and hybrid methods dating back to before the Cold-War? In answering this question, I will analyze Soviet military strategy and present day Russian military doctrine, focusing in particular on the case studies of Russian intervention in Estonia, Georgia and Ukraine to show that Russia still draws upon former Soviet doctrine in its cyber strategy. I intend to argue that Russia's use of cyber warfare in the information space is in fact a direct product of the continuity between Soviet and Russian military doctrine, thereby confirming the idea that while the West was still trying to frame cyber within a broader understanding of warfare in the twentieth century, the Russian Federation had already experimented with cyber during the 2007 cyberattacks on Estonia, and ultimately solidified its knowledge and techniques in the subsequent attacks on Georgia and Ukraine.

[10] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," 4.
[11] Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy."
[12] Gvosdev, "The Bear Goes Digital."

In laying out my argument, the first chapter will begin by exploring the inception of Soviet military thought. What concepts and ideas were the driving forces behind the formation of Soviet strategy? Specifically, I will look at the role of the offense-defense balance and the struggle the Soviets had in maintaining such a balance in their early doctrine, the effects of which are still to be felt in the present doctrine but subsequently allowed for cyber to be integrated into Russian grand strategy. I will ask, how did Soviet strategy ultimately lead to the formation of modern Russian military strategy? What about Soviet strategy lent itself to incorporating cyber under the umbrella term of information warfare in the Russian military doctrine of today? Furthermore, how do the 2010 and 2014 Russian military doctrines differ in their language regarding information warfare? Do the differences in doctrine coincide with the events in Estonia and Georgia? How did these attacks help shape the 2014 doctrine, which will be in effect until 2020?

In chapter two, I will continue to examine the questions posed in Chapter One, but in the context of the three case studies of Russian intervention in Estonia in 2007, the Russian-Georgian war in 2008, and finally the annexation of Crimea and subsequent military conflict and war in Eastern Ukraine. In each of the cases, I will outline the basic background information, the events of the attack, including the form of cyber attacks implemented, most importantly the DDoS or denial-of-service attacks that are seen across the board in each of the three cases and finally the implications of the attacks. How has Russia conceived of the different forms of cyber to its advantage? I will continue to look for evidence of continuity between the Soviet and Russian military strategies, while also looking for continuity of strategy between the three cases. I will examine the broader international response to the attacks, and Russia's counter- response. If Stuxnet is not, in fact, "Year One" as I contend, then how did the cyber attacks in Estonia help Russia reformulate its cyber doctrine and capabilities, and does the first attack on Estonia help us understand the successive attacks in Georgia and Ukraine? In addition, how did the amalgamation of asymmetric and hybrid methods first present itself in the Russian-Georgian war and again in the Ukrainian war? How do Russia's capabilities compare to the rest of the world, notably its two largest rivals, the United States and China? In exploring these questions, I hope to be able to definitively say whether Russia's use of cyber warfare, in the larger context of information warfare, is an extension of Soviet military strategy.

The study of Russia's use and implementation of cyber warfare as part of its modern military doctrine is important in trying to understand the multifaceted nature of cyber and reach an internationally agreed upon definition. More importantly, although Russia cannot stand for all authoritarian-leaning states, this thesis sheds light upon how the nature of cyber lends itself to flipping the traditional offense-defense balance, which assumes that the larger, more powerful, state is more likely to go on the offensive in an effort to take as much territory as possible. Instead, a state like Russia, which is not as powerful as its rivals the United States and China, can in fact engage in offensive strategic tactics to influence and alter the behavior of vulnerable, small, defense-driven states such as the border states of the Western alliance. Such an analysis allows us to understand how cyber plays a role in the offense-defense balance and, eventually, how cyber fits into the larger context of asymmetric and hybrid tactics.

Since the end of the Cold War, Russia has strived to regain and maintain its foothold as an important actor on the world stage. While the Cold War ended in the eyes of the world on November 9, 1989 with the fall of the Berlin Wall, and was further reinforced when other Soviet republics fell with the official collapse of the Soviet Union towards the end of 1991, the Cold War, one could speculate, did not end for everyone. Garry Kasparov[13], in 2015 published *Winter is Coming: Why Vladimir Putin and the Enemies of the Free World Must be Stopped*. He reflects on the fall of the Soviet Union from the perspective of someone who is a direct byproduct of the Soviet Union; having love for his country, yet challenged by deep reservations and provocative opinions about the present day Russian government and the decision-making of the West, led by the United States. Instead of focusing on the multipolar world that developed in the post-Cold War period, Kasparov highlights its faults in strategically addressing the shift in power after the fall of the Soviet Union:

> ...the winners were left without a sense of purpose and without a common foe to unite against. The enemies of the free world have no such doubts. They still define themselves by their opposition to the principles and policies of liberal democracy and human rights, of which they see the United States as the primary symbolic and material representative.[14]

While the West and the United States enjoyed their sweet victory over communism, the losers, or enemies of the free world, did not lose sight of their own positioning against the liberal and democratic values of the West. The euphoria of conquering evil felt real in the dismantling of oppression embodied in the fall of the Berlin Wall, but it did not mean that evil would just disappear.[15] Kasparov writes his book in the context of criticizing Putin's regime and as a warning to the West, describing Putin's relatively swift rise to power and consolidation of that power. Kasparov's point of view is important to consider in understanding the position Russia

[13] Famously known for maintaining the world champion status in chess for twenty years but also a writer, activist, and former opposition leader to Vladimir Putin.

[14] Kasparov and Greengard, *Winter Is Coming*, xi.

[15] Kasparov and Greengard, xx.

took following the Cold War, which also influenced the subsequent framing of its modern military strategy and helps to understand its actions taken against Estonia, Georgia and Ukraine. My goal is not to draw upon Kasparov from a purely academic perspective, but to use his voice of reason throughout my argument in an attempt to understand how the tumultuous political atmosphere following the end of the Cold War had just as much influence in forming Russian strategy in the 21st century and preparing the battlefield for the attacks to follow, as had Soviet military doctrine.

CHAPTER 1
The Continuity of Soviet and Russian Military Thought

In order to make sense of how Russian military strategy has evolved into its present form, one has to start by examining the history of Soviet military strategy. In this chapter we will examine the outset of Soviet military thought considering the concepts and ideas that became the driving forces behind Soviet strategy. Especially in regards to the hard fought effort to balance both the offense and defense, principally analyzing the language in relation to information (cyber) warfare and how do these discrepancies shed light upon Estonia in 2007 and Georgia in 2008 and ultimately begin to understand the continuum between Soviet and Russian military strategies.

Carl von Clausewitz, Prussian general and military theorist of the 18th century, influenced Soviet military leaders as well as future leaders of Russia. Clausewitz viewed the mobilization of the entire country for the good of the state, in both peace and war, as a necessity. As a result, the state would be able to protect its interests while also maintaining support and justification for its actions. The fact that Russian and Soviet strategists alike have drawn upon social mobilization to strengthen the state in preparation for war already points to continuity between Soviet and Russian military strategy. Byron Dexter, a reporter for the *Atlanta Journal* in the 1920s and Assistant Editor of *Foreign Affairs* magazine in the 1940s and 1950s, wrote in his article "Clausewitz and Soviet Strategy*,"* that Clausewitz' theories have been formative for Russian and Soviet military thought throughout the 20th century. In his examination of Clausewitz, Dexter discusses aspects of war in relation to social life and how war is essentially "an act of social life," not just the actions of 'little green men.' If war can be perceived as "an act of social life," it can also be regarded as a "political instrument."[16] One can posit that the way in which Russia views the nature of its cyber operations also has its basis in the theoretical ideas of Clausewitz, who promoted the theory of 'unified war', which grew out of the idea of mobilizing the whole state, "directed by a supreme intelligence, in which political and military instruments are used indifferently to suit a particular object in the pursuit of a gigantic plan."[17] While here Clausewitz is referencing the 'peace offensive,' this same idea can be applied to Russia's utilization and weaponization of information warfare. Under the Russian Federation, pursuing 'unified war' could now be seen as including information warfare, which is ultimately the 'gigantic plan," but which Clausewitz could not have predicted at the time.

Boris Shaposhnikov, a former Soviet military commander, Chief of Staff of the Red Army and Marshal of the Soviet Union, whose book *The Brain of the Army* famously sat on Stalin's desk, adopted many of Clausewitz' theories in the development of Russian military strategy and also influenced future leaders of Russia. Clausewitz' theory often aligned with Marxist ideology, acknowledging a connection between war and politics as reliant on one another for their success and effectiveness.[18] Though Lenin did not become a Clausewitzian scholar, fact of the matter is that he was able to read Clausewitzian theory from his perspective as a politician, as Dexter writes, rather than as a "military man," is key in talking about Russia's role in information warfare today. Beginning with Lenin, Russian military thinkers were able to conceive of politics, war and social life on the same plane. From the perspective of Dexter, this feature was unique to the Soviet, and now Russian, strategy: the ability to implement "a strategy of a new type, in which the entire economic, moral and military potential of the nation is enlisted

[16] Dexter, "Clausewitz and Soviet Strategy," 41.
[17] Ibid.
[18] Dexter, 44.

for the attainment of a clear and overriding goal."[19]Although a 'unified war' may not have included cyber war in the eyes of Clausewitz in the 18th century or in the eyes of Lenin or Stalin in the 20th century, it is clear that the creation of cyber as a tool or instrument for facilitating this grand plan of 'unified war' has only aided Russia.

Soviet military strategy devised as a result of the Bolshevik October Revolution of 1917 initially had the goal of expanding the revolution beyond the borders of the Soviet Union. Revolution would spark uprisings in the capitalist states, which in turn would lead these capitalist societies to embrace socialism. The Bolsheviks quickly realized this ambitious goal of waging a worldwide revolution was unattainable, alternatively resorting to protecting the revolution inside the borders of the newly formed Soviet Union. In the spirit of socialist ideology, the Bolsheviks set out to organize an entire army comprised only of volunteers, which would later become the infamous Red Army. In her book *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, Condoleezza Rice writes that this decision to protect the revolution within the borders of the Soviet Union was the most important decision the Bolsheviks made in the development of Soviet military strategy.[20]

In the formative years of the Soviet military, three main strategists arose to prominence: Mikhail Tukhachevsky, formerly a junior lieutenant in the imperial army, who held an imperial and Bolshevik perspective on war; Leon Trotsky, a Russian revolutionary, well-known theorist of Marxism and at the time the commissar of foreign affairs and war;[21] and Mikhail Frunze, a prominent Bolshevik leader during the 1917 Russian Revolution and a Red Army commander

[19] Dexter, "Clausewitz and Soviet Strategy," 55.

[20] Rice, Craig, and Gilbert, "The Making of Soviet Strategy," 649.

[21] "Leon Trotsky | Biography, Books, Assassination, & Facts."

during the Civil War. Each one made contributions to the formulation of Soviet strategy that have had a lasting effect on both Soviet and Russian military thought.

Concepts and Ideas as Driving Forces of Soviet Strategy

Each of the original framers of Soviet strategy contributed vastly different perspectives to the development of Soviet doctrine. As a result, although the doctrine may be considered to be sophisticated, it contains concepts that could be viewed as contradictory or underdeveloped. Mikhail Frunze drew upon the traditional values of peasant culture as well as on the revolutionary values of the proletariat. The reality of peasant life and proletarian life shared characteristics with partisan or irregular warfare; the peasant had no ownership of the land and was used to cultivating it with a limited amount of resources, while the insurgent nature of the proletariat accustomed it to asymmetric conflict. Frunze allied the mind of the peasant with the mind of the proletarian, and in that way envisioned combining partisan warfare with an offensive strategy.[22]

Frunze never had the opportunity to explain how offensive strategic thinking was to be implemented in the Soviet system, never specifically "clarifying whether the political offensive or the military strategy of the offensive was at the core of his argument."[23] This vagueness still exists in the offense-defense balance of Russian military strategy and thought today, where the political doctrine is defensive while its military strategy is offensive. Therefore, the implementation of cyber into modern doctrine has been relatively seamless, because as Rebecca Slayton writes in *What is the Cyber Offense-Defense Balance?* since according to

[22] Rice, Craig, and Gilbert, "The Making of Soviet Strategy," 653–55.
[23] Rice, Craig, and Gilbert, 658.

offense-defense theory, technology is perceived as favoring the offense,[24] it has therefore been natural for Russia to continue along the path of pursuing the offensive strategy through the use of cyber. An examination of the offense-defense balance of Russia would be the subject for another study, yet it is important to mention it here in order to understand how Russia has come to implement cyber as a part of its grand strategy.

Although Frunze wanted to work towards perfecting a strategy that would result in the formation of a "mass army,"[25] he also grudgingly understood the importance of accepting technological advancement for the development of future warfare. In order for the diplomatic, economic, and military sectors to function in a coordinated manner, knowledge alone would not be enough, as Trotsky argued, but also required a skill set, preparedness and the willingness to accept developments in military science. These ideas supported by Frunze were in fact originally put forth by Tukhachevsky.[26]

Mikhail Tukhachevsky and Boris Shaposhnikov, a Soviet military commander, Chief of Staff of the Red Army and Marshal of the Soviet Union, understood the value of having the support of the entire country as validation and justification of state actions in times of war and in times of peace; if worldwide revolution was not possible, then the future of socialism and the safety of the Union lay in the hands of the proletariat and the peasant. Learning from its failures during the Civil War, the Soviet government mobilized the economic system to protect and support the interests of the military, highlighting the importance of communication as a useful tool of support for the army. Tukhachevsky's prediction of the importance of the military

[24] "According to the offense-defense theory, state perceptions that technology favors the offense increase fears of attack, encourage arms races, and, through interactions between fears and capabilities, increase the likelihood and consequences of war." Slayton, "What Is the Cyber Offense-Defense Balance?," 72.
[25] Rice, Craig, and Gilbert, "The Making of Soviet Strategy," 656.
[26] Rice, Craig, and Gilbert, 662.

sciences, has come to fruition in present day Russian strategy as we see the fields of communications and military science collide in the cyber realm.

Before World War II, the Soviet Union had a significant military collaboration with Germany to develop the Red Army in logistical terms. Collaborating with a foreign army allowed for the Red Army to overcome its problem of depleted resources. Missing from Rice's account is the significant economic reason for this collaboration on the part of the Red Army. During the time of the collaboration, the Soviet Union was undergoing massive economic development through the implementation of the New Economic Policy between 1921 and 1928 imposed by Lenin. The policy represented a temporary loosening of the extreme centralization characteristic of wartime communism, and was subsequently replaced with Stalinism, which drove the country into a period of intense industrialization, surpassing the achievements of Germany.[27]

This understanding of the necessity and importance of technology was not specific to Frunze but was widely accepted, lasting into the Cold War Era. James J. Wirtz writes in *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy* that what Russians have generally lacked in technological expertise and innovation, they make up for "in their ability to foresee the broad impact of technology on the battlespace." In Frunze's time, the early Soviets were still trying to conceive of how to organize an effective army rather than focusing on technological development and innovation. This decision is definitely felt later during the Cold War era when much of Soviet cyber activity was centered around traditional

[27] Rice, Craig, and Gilbert, "The Making of Soviet Strategy," 668.

cyber espionage in an effort to obtain Western scientific, technical and military intelligence and be able to to compete, or as Wirtz writes, to "keep pace with more sophisticated and innovative opponents," and in that way they were able to overcome the lack of technological advancement offensively.[28]

Leon Trotsky, whose own form of Marxism has been coined Trotskyism, did not believe in a centralized doctrine as Frunze, but his ideas did not stray far from the offensive. While Trotsky and Frunze clashed over the idea of a formulated doctrine for the Red Army, both valued the importance of preparedness for military success. Trotsky once said that the only doctrine needed was to "be on the alert and keep your eyes open." More seriously, Trotsky argued that a formulated doctrine would "not only improperly formulate general goals, strategy, and tactics" but also "divert attention from most practical and vital tasks"[29] The Trotsky-Frunze debate became formative in the development of Soviet strategy in the following years. Ultimately, Frunze's argument of a centralized doctrine triumphed over Trotsky's of a loose uncentralized doctrine focused rather on skill, but the weakness of Frunze's argument, who never clarified if the offensive should take precedence over the political, or was only meant to be applied in the event of war, is still felt in Russian military thinking today.

While the Bolsheviks had wanted to create a worldwide revolution to promote communist ideology, Trotsky recognized the 'slippery slope' of creating a worldwide system of militarization to protect and benefit that revolution, (clearly in line with Marx's original vision). As Rice briefly notes herself, it could be argued that present day Russia has fallen into this trap without even trying to wage a worldwide Soviet Revolution. The regime has protected the

[28] Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," 31.
[29] Rice, Craig, and Gilbert, "The Making of Soviet Strategy," 656.

interest of the Russian state at all costs, and the way in which Putin has maintained his grip over Russia for the majority of the 2000s and 2010s, shows how a form of hybrid authoritarian power has usurped the legitimate mechanisms of the Federation. The anxieties first expressed by Trotsky have now become a reality for the Russian people, with the government giving the impression that the country is truly "encircled by hostile powers," thus instilling the "fear of internal enemies," into the minds of the citizens.[30] These fears were then exacerbated and emphasized by the 2008 economic recession, allowing the Kremlin and the Russian society more cause to feel undermined by the West.

The fear and paranoia over how to protect the integrity of the Union was not specific to Trotsky alone but also became a supreme concern under Stalin. Rice implies in her account that Stalinist military thinking combined with "Stalin's infallibility" made it difficult for Soviet military thought to progress.[31] While Rice calls it "Stalin's infallibility," it would be more correct to say that Stalin had a strong personal belief in his own infallibility. Stalin decided that officers and commanders loyal to Germany were to be deemed untrustworthy of the Soviet Union and therefore 'eliminated.' Crucial military thinkers, among them Tukhachevsky, were executed during the purge, and those who survived were silenced. As a result, the Red Army faced a massive challenge with the loss of so many excellent military minds, therefore Soviet military thought stagnated and was overshadowed by Stalinism. Soviet military history at this juncture should be stressed because it solidified Russia's drive towards the offensive based on the fear and paranoia conceived by Trotsky and achieved by Stalin through the purges. As a result, in lieu of the regime directing its fear and paranoia against the actual "hostile powers," which it so feared,

[30] Rice, Craig, and Gilbert, "The Making of Soviet Strategy," 660.
[31] Rice, Craig, and Gilbert, "The Making of Soviet Strategy," 664.

the fear and paranoia was directed inwardly and became a detriment to Soviet goals instead. This offensive strategy driven by fear must be taken into account in regard to Russia's use of cyber today.

Unable to keep pace with Stalin's chokehold over Soviet military thinking, and together with the inability to define Frunze's vague argument about the offense-defense balance, the underdeveloped character of Soviet strategic thinking became more apparent during the Winter War waged against Finland from 1939-1940, in which the Red Army won, but left with heavy losses in numbers. Stalin became a threat to the state he so wished to protect because of his own obsession with loyalty to the Union and maintaining his own power. The Molotov-Ribbentrop Pact of 1939 was key for Stalin in the interest of saving time and enabling the Soviet Union to situate itself militarily. The infamous pact determined on paper how the Russian and German spheres of influence could peacefully coexist, but in turn placed the futures of Poland, Finland and the Baltic States in jeopardy,[32] which is important for our discussion of the three case studies discussed in the next chapter. The way the Soviets ultimately won the war was through the effective mobilization of the Soviet state. In addition, they were able to draw upon the hidden strength of their vast expanse of territory.[33] The Red Army struggled over the course of the war, but their tactics improved as the army's adaptability aided the army effectively even when resources were scarce.[34]

After 1942, more attention was paid to the importance of defense, though offense continued to be regarded as the main form of combat. The Soviets tried to reimagine defense as a tactic that can be as mobile as the offense when it is part of an overall mobile warfare strategy;

[32] Rice, Craig, and Gilbert, "The Making of Soviet Strategy," 670.
[33] Rice, Craig, and Gilbert, 671.
[34] Rice, Craig, and Gilbert, 672.

once they had improved upon their defensive strategy, they could finally employ their offensive strategy more effectively and with more confidence.[35] This reimagination of Soviet strategy became crucial in developing Russia's cyber capabilities in the 21st century, by virtue of the fact that the cyberspace has allowed Russia to maintain the offense as their predominant form of strategy, while also flexing their defensive muscle allowing for increased mobility. What the Soviets ultimately learned in World War II was the importance of defense -- an army cannot have an effective offense without an effective defense to rely on. They were able to reconfigure after the first half of the war and adjust their strategy temporarily, in accordance with the changing battlefield. These adjustments to strategy were only successful due to the support and mobilization of the entire Soviet state.[36]

Moving forward, the roles of the offense-defense balance, mobilization of the state, and the peasant and proletariat as a the motivation behind advancing asymmetric and hybrid methods on the battlefield, where the most significant points in ultimately influencing Russian military doctrine. In Terry L. Heyns' *American and Soviet Relations since Detente*, he lays out the intrinsic differences between both societies and political systems. In the Soviet era, technology and media were perceived as only worthy when placed in the context of supporting the Soviet regime, where in contrast to the United States, technology and media were used as a form of commercialization in support of the economy. As a result, the same way Russian military strategy stagnated after the Stalin's military purges, the Soviet hesitation of accepting technological advancements during the Cold War (minus the Space Race with the United States, which was purely an extension of the ongoing arms race) it is is surprising when in hindsight

[35] Rice, Craig, and Gilbert, "The Making of Soviet Strategy," 672.
[36] Rice, Craig, and Gilbert, 673.

Tukhachevsky and Frunze alike, fundamental to Soviet military thought, had stressed the importance of accepting technological development as Soviet military strategy. This may explain why Russia's cyber capabilities had not been fully developed up until Estonia, because the West assumed that such capabilities were not possible in regards to a state that has historically been hesitant technological growth.

Russian Military Doctrine(s) as an Extension of Soviet Military Strategy

Since the 2007 Estonian cyber attacks, the Georgian, the annexation of Ukraine in 2014, and the 2016 U.S. presidential election, Russia has made increasingly aggressive advances on the world stage to legitimize its standing while also countering the West. Amid these confrontations, Russia has also been quietly maximizing its cyber capabilities and integrating these capabilities into a larger structure of information warfare and strategy. Russian military thinkers have coined the term "New Generation Warfare," to describe how Russia is shifting from the battlefield of traditional warfare that dominated the 20th and 21st centuries and bringing war into the cyber realm in order to achieve the ultimate goal of "contactless war."[37] Russia's objectives for achieving this contactless war are explored throughout the two versions of the modern doctrine, published first in 2010 and then revised and republished in 2014. It is important to note that the Russian government's list of definitions of terms such as *military security*, *threat*, *danger*, *military conflict* and *armed conflict* are all formulated to reflect the point of view of the Russian government and military. It does not mean that these are internationally agreed upon definitions

[37] Bērziņš, "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy," 5.

of these terms. The definitions are mostly identical between the two doctrines, other than the addition of "mobilization readiness of the Russian Federation" in the 2014 doctrine:

> (l)...the ability of the Armed Forces, other troops and organs of the economy, state and federal authorities, public authorities or subjects of the Russian Federation, local governments and organizations to implement mobilization plans.[38]

Mobilization, as stated by this clause, is not specific to the Russian government or to the military, but instead is expected of the state as a whole, reminiscent of Soviet military thought. The strategy of mobilization was used in preparation for World War II in an effort to consolidate depleted resources, whereas now this strategy is implemented in order to have total control of all state sectors. While under Soviet strategy mobilization of the state was proposed as a strategy that would hypothetically benefit the state in preparation for war, it is evident in this clause that it is the role of the military to mobilize all necessary sectors. This centralization and rallying of the state is important in relation to cyber because it means that cyber is in effect included in the strategy of total mobilization as well.

In Connell and Vogler's examination of *Russia's Approach to Cyber Warfare,* they describe Russia as perceiving the information landscape to be a separate domain of war, which allows the state to dominate this landscape both domestically and internationally. Similar to the Chinese, Russians use the broader term *informatization,* rather than cyber (or *kiber*), which is commonly used in reference to the West. Russians conceptualize any cyber operations as part of a larger structure of information warfare or *informatsionnaya voyna*.[39] *The Military Doctrine of the Russian Federation* (2010) states that the purpose of information warfare is to achieve a

[38] "The Military Doctrine of the Russian Federation (2014), 2."

[39] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," 3.

political objective without the use of military force, while also shaping the discourse regionally and internationally in favor of the Russian Federation. The umbrella term of information warfare emcompasses computer network operations, electronic warfare, psychological operations, and information operations. It includes the now infamous disinformation campaigns on social media during the run-up to the 2016 U.S. presidential election, as well as troll farms[40] fueling those campaigns, together with more subversive campaigns, such as cyber attacks affecting both the psychological and physical infrastructure of their adversaries, both regionally and internationally. Listed within the Military Doctrine are Russia's main tasks for deterrence and a description of the military conflicts in which these information technologies are to be used as a way of advancing the Federation's relations on the global scale as well as regionally:

> information technologies are used as a way to assess and predict the development of the military-political situation at the global and regional level and also the state of interstate relations in the military-political sphere…[41]

The inclusion of this clause alludes to the Soviet goal of minimizing the physical use of force in times of war. In the context of modern Russian strategy, shaping the discourse is achieved through the use of information technologies (cyber) to monitor the general "military-political situation." As Kasparov points out, if the government has control of the so-called "fourth estate," e.g., the news and media, the government will also have control of the other three.[42] Although the

[40] "Trolls" are traditionally known for online bullying called "trolling." But the terms has taken on a larger meaning in the context of Russia in relation to groups of people or "farms," who engage in trolling as a way of inciting distrust and uncertainty in their targets. Professor Whitney Phillips explains that "trolls take perverse joy in ruining complete strangers' days." Ultimately, Phillips writes, "trolls are motivated by what they call *lulz*, a particular kind of unsympathetic, ambiguous laughter." They're in it for fun, even if a sickening form of fun that comes at others' expense. And trolls are fundamentally disorganized: They act as a flash mob, grouping together spontaneously to troll different targets and then going their own way." Geltzer, "Stop Calling Them 'Russian Troll Farms.'"

[41] "The Military Doctrine of the Russian Federation (2010), 7"

[42] Kasparov and Greengard, *Winter Is Coming*, 10.

fourth estate does not include cyber, the fact is that the information technologies, which do include cyber, can be appropriated as a way of controlling the fourth estate, which in turn is manipulated to influence the discourse of society, whether at home or abroad.

Col. S.G. Chekinov (Res.) and Lt. Gen. S.A. Bogdanov (Ret.), two Russian military specialists on information operations, point to the general Russian theory of cyber operations, in which information has the power to "disrupt governance, organize anti-government protests, delude adversaries, influence public opinion, and reduce an opponent's will to resist."[43] The clandestine nature of cyber allows for both sides of a conflict to benefit from these operations. The antagonist can use cyber to achieve the goals of disruption and delusion, while at the same time the victim of the operations can organize counteractive measures using information technologies, in its turn influencing public opinion and even attempting to "delude" the antagonist and adversary when useful. However, it is an accepted axiom that in any cyber conflict it is the side with the superior means and capabilities that will be able to dominate. As a result, the government that does have the means will attempt to maintain some level of "plausible deniability,"[44] the term used when top officials deny any responsibility for wrongdoing by lower-ranking officials, through the manipulation of information technologies. Plausible deniability arises as a key issue and point of contention when addressing the role of responsibility in Estonia, Georgia and Ukraine.

Importantly, the 2010 doctrine does not identify information and communication technologies as one of the external threats to Russian sovereignty. In contrast, the revised

[43] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," 4.

[44] Plausible deniability, in relation to the state, can be defined as having the ability to deny any knowledge of, or responsibility for, wrongdoing, which can not be proved due to a lack of evidence.

doctrine of 2014 has added information and communication technologies under “main external military dangers”:

> (k) the use of information and communication technologies in the military-political purposes for acts contrary to international law, aimed versus sovereignty, political independence, territorial integrity of states and threatening international peace, security, global and regional stability.[45]

It must be noted that the language used here, e.g., “military-political purposes,” has direct ties to past Soviet military thought. Soviet military strategy, as Rice writes, could be defined as having two distinct parts: on the one hand the political-military, “which attempts to define the purpose and character of military power,” and on the other hand the military-technical side, “which determines how Soviet military will operate in the field.”[46] The language found in the doctrine echoes this dichotomy of the political-military versus the military-technical aims of strategy. The focused use of information and communication technologies is aimed at aiding the political-military side, first and foremost. The technologies, in the case of Russia, have often been placed in reference to sovereign and territorial integrity, drawing upon Berzins’ conception of Russian military doctrine as having two distinct parts, those being: “doctrinal unilateralism” and “legalism.”[47] Berzins writes that a legal framework which supports and above all justifies the actions of the state, also allows a role for plausible deniability. By explicitly stating that the Russian government supports the use of these technologies “contrary to international law,” it is clear that the Russian government implements cyber policy according to its own interpretation of international law. This explains how Russia can justify its actions in Estonia, Georgia and

[45] “The Military Doctrine of the Russian Federation (2014), 3.”
[46] Rice, Craig, and Gilbert, “The Making of Soviet Strategy,” 663-64.
[47] Bērziņš, “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy,” 3.

Ukraine; therefore according to its own interpretation of international law there was no wrongdoing.

Both the 2010 and 2014 doctrines equally outline significant features of contemporary forms of warfare or conflicts crucial to the understanding what direction Russian military strategy will take in the future. The first notable clause in the section outlining "characteristic features of contemporary military conflicts" reads: "the integrated utilization of military force or forces and resources of a non-military character,"[48] highlighting further consolidation of the army and the use of non-military means to advance the military and political agenda. Drawing upon the importance of mobilization of the military and how mobilization will continue to be important going forward. This alludes to the character of cyber in which the offensive is favored, therefore, the Russian military seems to acknowledge this fact by including this clause. Yet, in the revised 2014 version of the document, the language has been revised in plainer terms:

> (a) integrated use of military force, political, economic, information and other non-military measures nature, implemented with the extensive use of the protest potential of the population, and special operations forces[49]

Integration is affirmed even more strongly than in the 2010 doctrine, another sign that present day Russian doctrine echoes Soviet military thought in drawing upon mobilization as a means of supporting the military while also protecting the state. The 2014 clause is unique to this document in inserting "protest potential," echoing Soviet military thought as well. The Russian state continues to value the mobilization of the people in support of state actions, another point that establishes a continuum. Furthermore, in the 2014 version, the language has been clarified to

[48] "The Military Doctrine of the Russian Federation (2010), 5."
[49] "The Military Doctrine of the Russian Federation (2014), 4."

stress the integration and synchronization of information with military force, together with the political and economic spheres, and other non-military measures. While, in the 2010 version, the Russian government predicted information warfare could have an impact based on its experience with the conflicts in Estonia and Georgia, it is clear that the revised and clarified language of the 2014 document indicates that the focus on information warfare is increasing, and embodying itself in the doctrine. Another important addition, the " (i) use of indirect and asymmetric methods"[50] which are to be further explored and employed, connects to Soviet military strategic thinking as its basis, but in addition expands the doctrine to apply to present-day strategic norms in order to be competitive in the 21st century. The document implies that the Federation has explored these methods in the past, but with the explicit addition of information (cyber) warfare and technologies into the doctrine, it can be understood that cyber warfare is seen by the Russian government as an extension of asymmetric warfare by other means.

In addition to treating the role of mobilization, clause (c) from the 2010 version draws attention to troops and resources, and the scale at which they are used in the airspace and outer space domains -- the document mentions only two out of four domains, the other two being land and sea.[51] This may point to the fact that airspace and outer space at the time were a priority for development in order to make these domains more competitive. The 2014 version clarifies the clause as: "the effect on the enemy throughout the breadth of its territory simultaneously in the global information space, aerospace, land, and sea."[52] There has been a significant shift from the 2010 to the 2014 doctrine, with the latter version citing the importance of infiltrating the enemy in all of its domains — including the information space — in order to defeat the enemy. It is

[50] "The Military Doctrine of the Russian Federation (2014), 4."
[51] "The Military Doctrine of the Russian Federation (2010), 5."
[52] "The Military Doctrine of the Russian Federation (2014), 4."

logical that this would be included in the 2014 doctrine, as the government learned from its successes in Estonia, and then put its techniques again into practice in the war with Georgia, in 2008, and finally in Ukraine, where the conflict began, conveniently, in 2014. This leads me to believe that this clause was improved upon in order to provide support and justification for Russian government actions in neighboring countries through "legalism," as argued by Berzins.

One of the more important clauses in the 2010 doctrine may possibly be clause (d) under "the characteristic features of contemporary military conflicts," directly addressing "the intensification of the role of information warfare."[53] It is clear that the biggest difference between the two doctrines can be found in the two parallel sections entitled "characteristic features of contemporary military conflicts" and "features of modern military conflicts" in the 2010 doctrine. In the 2014 doctrine, this distinction is not made: instead, the two sections are compiled under the one heading "the nature and characteristics of modern warfare," which integrates information warfare throughout the clauses. It is clear from this particular clause that information warfare is to be implemented (a) for achieving political objectives, (instead of using military force) and simultaneously (b) to change the response of the world community towards Russia's actions and therefore minimize judgement. This demonstrates that in 2010, the Russian government had a significant interest in actualizing information warfare as a part of strategy and conceptualizing *how* to implement it into present day strategy. In stark contrast, the 2014 doctrine has completely eliminated the former clause, which has been changed to: " (d) selectively and a high degree of destruction of objects, speed maneuver and the fire, the use of various mobile groups of troops."[54] The 2010 clause has been completely replaced to instead

[53] "The Military Doctrine of the Russian Federation (2010), 5."
[54] "The Military Doctrine of the Russian Federation (2014), 4."

highlight the mobility and destructive potential of troops, providing evidence of another important shift between 2010 and 2014. Not only has information warfare been integrated into several clauses in the 2014 version of the doctrine, but information warfare itself has been implemented in Russian strategy and in real, physical terms in the Russian military.

Contrary to the 2010 doctrine, the 2014 doctrine has four entirely new clauses added to the end of the section addressing characteristics of modern warfare. These clauses were added possibly as a response to the progression of conflicts between 2010 and 2014, proof that information warfare was being actualized in the strategy itself:

> (g) the creation, in the territories, of the warring parties' permanent war zone…(h) participation in hostilities, irregular armed groups and private military companies…(i) the use of indirect and asymmetric methods [of] action…(j) the use of externally funded and run political forces and social movements[55]

These four consecutive clauses directly address asymmetric and hybrid conflict with emphasis on the irregularity of armed groups, territories in a state of constant conflict, the increasing role of social movements involved in conflict, and, most importantly, accentuating the growing importance of "indirect and asymmetric methods." This depicts the fact that the Russian government recognizes that asymmetric and irregular methods will and have already played a more significant role in modern warfare.

In listing these clauses, the document implies that the Russian government is *willing* to engage in asymmetric and hybrid conflict. The existence of these clauses solidify my claim that Russia has always engaged in asymmetric and hybrid methods of conflict since the inception of Soviet military strategy, and displaying a continuity between the doctrines. These clauses are

[55] "The Military Doctrine of the Russian Federation (2014), 4."

reminiscent of Frunze's early discussion of the dichotomy between the offensive and defensive characteristics of the proletarians and peasants, and the further manifestation of these characteristics in Soviet strategy. The clauses are also evocative of Berzins' argument that Russia has a pattern of utilizing legalism to condone its actions. These irregular methods have a direct connection to Russia's use of offensive and defensive strategy and the development of Russia's present day cyber capabilities.

This chapter has attempted to demonstrate the continuities between Soviet and Russian approaches to warfare, with a particular emphasis on asymmetric and hybrid forms of warfare. We have seen how there is a clear continuity between Soviet and Russian strategy, apart from this, the differences between the 2010 and 2014 doctrines provides evidence that these differences mirror the succession of events between Georgia and Ukraine specifically. In the next chapter, we will focus on how Russia's actual use of cyber has evolved since the first attack on Estonia in 2008 to demonstrate the realization of evolving military strategy throughout the consecutive attacks on Georgia and Ukraine.

CHAPTER 2
The Cyber Inception

The post-Cold War days of a unipolar world, in which the United States dominated the international power politics, is not over *per se,* but definitely on the decline. The Russian Federation feels threatened by the direction world development is taking, increasingly accepting of nations competing for superiority on the world stage, resulting in multipolarity among states on the international level. *The Military Dangers and Military Threats to the Russian Federation,* stresses changes in world development such that other nations are reaching for "all-embracing domination" and multipolarity. However, these developments have only benefited Russia, which has taken the opportunity to re-establish its circle of influence in the post-Soviet bloc. The irony of it is that Russia is exactly one of the countries doing just that: attempting to compete with other world powers. While in the Soviet era, ignoring the international system worked in favor of maintaining the revolution within the borders of the Union, the same strategy would not be able to work in the post Cold-War era having been embraced by the West and invited to participate in the international system. In the eyes of the West, inviting the new Russian Federation to the table was a way of saying let bygones-be-bygones and hopefully by being integrated into the international democratic system would enable the Federation to democratize.

In talking about the three cases of cyber attacks in Estonia, Georgia and Ukraine and returning to the contemporary Russian military doctrine, Russia views of "(e) territorial claims against the Russians Federation and its allies and interference in their internal affairs"[56] as one of their main external dangers to the Russian Federation. This clause remains unchanged in the 2014 revised doctrine seemingly acknowledging the conflict with Georgia in 2008 and the

[56] "The Military Doctrine of the Russian Federation (2014), 3."

international community's response, which returns to Berzins' point about Russia's use of legalism to justify its actions, especially internationally. Moreover, this clause also acknowledges Trotsky's prediction of a Soviet Union "encircled by hostile powers and so fearful of internal enemies that it would be brutally repressive,"[57] in the event that worldwide revolution fails. Though Trotsky never clarified what he meant by 'hostile powers', I could argue that these "hostile powers" in the present day are NATO and the European Union, especially in reaction to Russia's increasingly aggressive presence in the international space. This feeling of reestablishing its sphere of influence has lately become a large point of contention, in which Putin has tried to establish a so-called Monrosky doctrine, a sort of parody of the American Monroe doctrine, of protecting the Russian sphere of influence by advocating for ethnic Russian populations in much of the post-Soviet bloc. While the above clause (e) addresses Russia's anxiety over the global perception, the subsequent clauses (h) and (i) clarify Russia's positioning, this time in relation to conflicts bordering Russia:

> (h) the use of military force on the territories of states contiguous with the Russian Federation in violation of the UN Charter and other norms of international law…(i) the presence of seats of armed conflict and the escalation of such conflicts on the territories of states contiguous with the Russian Federation and its allies.[58]

The Russian government feels not only pressure from the international community and institutions such as NATO and the E.U., but also from the bordering states in which Russia has interests in both their ethnic Russian base backing the Kremlin and those staunchly against the Kremlin and westward leaning. These clauses seem to address Russia's positioning on the

[57] Rice, Craig, and Gilbert, "The Making of Soviet Strategy," 661.

[58] "The Military Doctrine of the Russian Federation (2014), 3."

incidents in Estonia and Georgia, but definitely also the conflict underway in Ukraine, at the time in 2014, which has brought Russia into a negative spotlight on the world stage.

In this chapter, we will continue to consider the questions posed in Chapter 1, yet in the context of the three cases studies of Estonia (2007), Georgia (2008) and Ukraine (2014). In considering each of the cases, I will summarize the basic background and history, events of the actual cyber attacks, as well as look at the specific types of attacks used in each of the cases. Additionally, we will continue to look for points of cohesion between Soviet and Russian strategies, while also look for the continuity of mobilization, the presence of offense-defence and the relationship of asymmetric and hybrid warfare in Russian strategy throughout the three cases.

Part 1: Estonia (2007)

Essential Background

Following the independence of the Baltic nations, Latvia, Lithuania and Estonia, their governments have actively worked to dismantle, displace or replace Russian and Soviet statues in prominent public locations. In Latvia, already after the First World War, the statue commemorating Peter the First, dating from the Russian Empire, was torn down and replaced by the Freedom Monument in 1935 commemorating the Latvian troops who died in the War of Independence from 1918-1920. Having survived almost 50 years of Soviet occupation, today the monument still stands overlooking Old Town Riga, viewed as an important symbol of freedom and prosperity and used as a point of gathering. Lithuania, too, has taken significant and sometimes extreme strides to eliminate Soviet statues from public spaces. Most remnants of statues have been moved to Grutas Parkas or "Stalin World," essentially an entire park devoted to old Soviet statues.

In early April of 2007, following the March parliamentary elections, the conservative Estonian government of Prime Minister Andrus Ansip, made plans to move the controversial Bronze Soldier from Tónismägi Park in central Tallinn to the remote Defense Forces Cemetery. For many Baltic people, Soviet statues have represented the Soviet oppression under which they lived for 50 years. On the other hand, the ethnic Russian population in Estonia viewed the Bronze Soldier as a symbol of their own. The statue commemorates the Soviet liberation of Estonia from the Nazis on April 30th.[59] The Kremlin expressed that the displacement of the statue infringed on the rights of their ethnic Russians and that Estonia would pay the consequences of its displacement.[60] This increase in social tensions led to protests and riots in the streets by the ethnic Russian population. These protests were appropriately dubbed the "Bronze Night" protests.[61] Meanwhile in Russia, a youth group demonstrated against the Estonian ambassador and attacked the Estonian Embassy in Moscow. Most of the protests in Russia were led by the government funded pro-Kremlin "Nashi su" or "Youth Movement, Ours!" Established in 2005, this anti-fascism student group now has more than 100,000 members.[62] The riots outside the embassy did not cease until the ambassador left Russia after a deal was struck with Germany, but there have been conflicting accounts about whether the ambassador was attacked. In addition, the Russian government even suspended rail service between Tallinn and St. Petersburg.[63]

[59] Herzog, "Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity," 68.
[60] Kampmark, "Cyber Warfare Between Estonia and Russia," 288.
[61] Herzog, 68.
[62] Shackleford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," 206.
[63] Herzog, 7.

The Attacks

The cyberattacks first began at 11 pm local time on Tuesday, May 8th but were alleviated by 7 am the next morning. Even so, the attacks were still visible in traffic logs 30 days after the initial attack.[64] The attacks culminated on May 9th, which is coincidentally a symbolic day for Russians, called May Day, a day to remember their victory over the Germans in World War II.[65] According to Bill Woodcock and Ross Stapleton-Gray of Packet Clearing House, a nonprofit research institute for Internet traffic exchange technology, this particular time frame, together with the unique signature of *botnets*[66] that were used, indicated that the perpetrators may have been the Russian Business Network[67] based on some of their previous spam-sending campaigns. Woodcock and Stapleton-Gray drew the conclusion that the attack must have been a "one-month attack for hire" or was made to imitate one. The attackers took down Estonian government websites as part of a large DDoS (distributed denial-of-service attack).[68] While the DDos waged its destruction on Estonian internet infrastructure, Vladimir Putin released his own statement in response to the relocation of the Bronze Soldier: "Those who desecrate monuments to the heroes of the war are insulting their own people and sowing discord and new distrust between states and people."[69]

Among the websites affected by the attacks were those of the Estonian parliament, the national defense minister, as well as of Prime Minister Ansip's political party and a number of

[64] Stapleton-Gray and Woodcock, "National Internet Defense---Small States on the Skirmish Line," 51.

[65] Ashmore, "Impact of Alleged Russian Cyber Attacks, 7."

[66] Botnets are previously hacked computers, at any location, that have the ability to send out information that overwhelms an internet server.

[67] RBN is a multi-faceted cybercrime organization specializing in identity theft, which happens to be based out of Riga, Latvia, which has been speculated to have ties to the Russian government but has never been proven.

[68] A distributed denial of service attack is defined by Ashmore as "a cyber attack that disrupts internet service so that a user cannot access a given computer service."

[69] Herzog, "Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity," 69.

major universities and national newspapers. Estonia's largest bank, Hansabank, had to temporarily cease online services while 97 percent of the population, who rely solely on online-banking, had no access. In addition to the larger DDoS and botnet attacks, the perpetrators also used "mail-bombing" -- using hacked emails to overload servers and shutdown the internet. BBC reported that several websites had been defaced with images of Soviet soldiers and quotes from Martin Luther King Jr. The perpetrators also used another method called "war dialing," automated phone calls directed at a company or institution, which had the effect of blockading all government and parliament offices.[70]

It is important to understand that Estonia is the most wired and technologically advanced society on our planet. Ninety percent of Estonians have easy access to broadband Internet and nearly 100 percent of their youth population are connected to the Internet.[71] Estonia has the second highest number of mobile phone subscriptions, following the United Arab Emirates. Each person in Estonia owns at least one gadget - approximately 188.2 devices per 100 people. In addition, free internet access is considered a basic human right therefore almost every feasible activity is done online from live-streaming to e-voting and even e-government.[72] For this to be possible, internet providers have found Estonia to be a perfect environment for an IXP or an Internet exchange point. An IXP essentially connects a community of internet service providers or ISPs. Some countries, such as the U.S. has more than one, Germany, on the other hand, has one large, concentrated IXP, but one city could also have multiple IXPs, such as Tallinn. Having these two IXPs was largely what saved Estonia from a complete internet collapse. Estonia has several privately controlled data circuits with connections to countries with whom they are

[70] Grassegger and Krogerus, "Weaken From Within," 19.
[71] Herzog, "Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity," 72.
[72] Laasme, "Estonia: Cyber Window into the Future of NATO," 59.

diplomatically aligned, and with whom Estonian ISPs have commercial relationships, such as Scandinavia and Western Europe ISPs. At the time of the attack, Estonia was able to receive aid from these ISPs in neighboring countries.[73] In addition, during the time of the attack, three internationally renowned IT experts were visiting Estonia at the time: Kurtis Lindqvist, CEO of Netnod Internet Exchange, Patrik Fältström, senior consulting engineer with Cisco and the cyber security advisor for the Swedish government, and William Woodcock, research director of Packet Clearing House and member of the board of directors of the American Registry of Internet Numbers.[74] Using their years of expertise, they found that the perpetrators of the attack were likely located in Estonia.

While this attack may not have hurt other countries to the same degree, considering the connectivity of Estonia, the attack paralyzed much of the country for days. Due to the fact that most news sites were compromised, it was impossible to spread news of the attack to the outside world, which is why the event was not as widely reported. While Estonia's internet is their greatest achievement, this attack proved that Estonia's e-system has the potential to also be its downfall and weakest point.

Implications

There continues to be a great debate about who were the perpetrators of the attack. Following the attacks, the Estonian government immediately blamed the Kremlin for funding the attack but because of the nature of the attack, it was hard to place blame without sufficient evidence. The European Commission and NATO conducted their own investigations and their technical experts were "unable to find credible evidence of Kremlin participation in the DDoS

[73] Stapleton-Gray and Woodcock, "National Internet Defense---Small States on the Skirmish Line," 52.
[74] Laasme, "Estonia: Cyber Window into the Future of NATO," 59.

strikes."[75] They came to this conclusion even though NATO officials alleged that "the attacks were beyond non-state actor capacities" implying that even if the Kremlin wishes to point fingers at individuals to alleviate responsibility, it is evident that these capabilities were more complexly conceived than that of a hacktivist.[76] Though the evidence is inconclusive, it is clear that from the very beginning Russia had an obvious political motive in rejecting the relocation of the Bronze Soldier statue and had firmly supported the rights of the ethnic Russian minority.

Peter Pomerantsev, author of *Nothing is True and Everything is Possible: The Surreal Heart of the New Russia,* states that "the Russian theory of war allows you to defeat the enemy without ever having to touch him." This theory happens to fit together like a puzzle piece with the nature of cyber warfare, which also allows the perpetrator to conduct significant damage on a system from any location, never having to face the consequences. Grassegger and Krogerus express this perfectly by pointing out that cyber warfare is more than just a series of hacks and "cyber riots," as some have called the Estonian incident, but "it is psychological manipulation, executed with targeted digital information designed to weaken a country from within. Estonia was an early experiment in that theory."[77]Following the events that played out in Estonia, Russia has applied similar tactics in subsequent cyberattacks in Kyrgyzstan and Georgia only a few years later. Estonia was in a way the guinea pig - if an attack could be successful in Estonia, the most tech-based society on our planet, it could work anywhere in the world.

Though no one has ever claimed direct responsibility for the attacks, there is some speculation that the Russian youth group "Youth Movement, Ours!" may have been behind the attack. Evidence has suggested some of the early salvoes may have originated from Russian

[75] Herzog, "Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity," 69.
[76] Ibid.
[77] Grassegger and Krogerus, "Weaken From Within," 20.

government computing centers or centers run by “Nashi su,” but no one has ever come forth to confirm or deny.[78] The Estonian government found great difficulty in convicting someone based on the laws that existed at the time. Estonian laws of the period stated that “certain surveillance and investigation procedures of suspected crimes of a conviction would result in fewer than three years’ imprisonment.” At the time, cybercrimes, including this attack, fell under this general law. Even so, the Estonian government managed to convict and fine a 21 year old ethnic Russian living in Tallinn, Dmitri Galushkevich, in relation to the DDoS attacks. He received no jail time but was fined approximately $1,650 for blocking the website of Prime Minister Ansip’s political party.[79] This conviction highlighted the need for a rewriting of the Estonian penal code. The penal code was revised to encompass criminal offenses, specifically using computers, and added sections to include offenses dealing with cyberattacks and cybercrime.

Revising the penal code is not the only step that Estonia has taken since the attacks in order to confront the consequences of living in a heavily digital world. Not only was the incident important for Estonia to understand what steps needed to be taken concerning cyber security, but it alerted other countries within the NATO alliance. In May 2008, Estonia along with Italy, Spain, Slovakia, Germany, Lithuania, Latvia, and the Allied Command Transformation, called for the establishment of a Cooperative Cyber Defense Center of Excellence (CCDCOE), appropriately located in Tallinn.[80] The establishment of the center is possibly the largest achievement by Estonia, with the help of the world community, in response to the cyberattacks. With the establishment of the center, member states are now able to educate themselves about cyber

[78] Shackleford, “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law,” 207.
[79] Herzog, “Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity,” 71.
[80] Laasme, “Estonia: Cyber Window into the Future of NATO,” 61.

defense and security through training and public outreach, as well as research and development.[81] Each year, CCDCOE hosts "Locked Shields" in which member states come together for the world's largest cyberwar exercise. In addition, CCDCOE also has hosted several conferences and symposiums such as the Cyber Conflict Legal and Policy Conference in September of 2009, which explored cyber conflict management.[82] By establishing this center in Tallinn as a cyber hub and hosting annual events such as "Locked Shields", Estonia has become the world leader on cyber security issues - reaffirming its reputation as "E-Estonia." In addition, in 2013 NATO established a second research center specializing in strategic communications called StratCom in Riga, Latvia, as well as a third center located in Helsinki, Finland focusing on "hybrid threats."[83]

A second achievement in the wake of the 2007 cyber attacks is the *Tallinn Manual on International Law Applicable to Cyber-warfare* written in 2009 by 20 security experts, legal scholars and academics. The manual came to be a non-binding document, which addressed legal questions surrounding digital conflict. The conclusion was drawn that "the definition of war appears to function online in much the same way it does offline."[84] This manual has in a way become the language of international cyber law and has brought attention and awareness around cybersecurity into the international realm. Just as the CCDCOE works towards tangible change on the physical level, the *Tallinn Manual* has changed the conversation around cyber for at least the next period of years. Hopefully, the *Tallinn Manual* can be a precursor of wider change on the international level and assist NATO and the UN in finding a way to reform their legal framework and develop a cohesive cybersecurity strategy.

[81] Laasme, 61.
[82] Laasme, 62.
[83] Grassegger and Krogerus, "Weaken From Within," 22.
[84] Ibid.

Part 2: The Russian-Georgian War (2008)

Background

The conflict in 2008 was focused on what is internationally recognized as the northern Georgian territory of South Ossetia and Abkhazia and their separation from Georgia. South Ossetia historically has had close ties with Russia, sharing a border with the Russian region of North Ossetia. About 70,000 South Ossetians are neither ethnically Georgian or Russian but rather are a distinctive ethnic community sharing a spoken language similar to Farsi. Due to the close proximity to Russia, most South Ossetians hold Russian passports. With the ruble as the main form of currency and receiving a $30 million annual budget, South Ossetia shares significant economic ties with the Kremlin.[85] Most importantly, Gazprom, Russia's state-owned gas company, is immoderately invested in the region with gas pipeline infrastructure connecting South Ossetia to Russia.

History of the conflict

The modern history of this conflict starts in 1991, when South Ossetians and Georgians fought over the control of the region. Though South Ossetians appeared to have considerably less military resources compared to Georgian forces, they received continual support from the Russian government, which allowed the conflict to persist. In 1992, the sides reached a ceasefire between both sides and South Ossetia was declared as an independent region within Georgia. Following the establishment of South Ossetia as an independent region, an identical war was fought in 1993, this time in the northwest region of Abkhazia, in which a similar agreement was

[85] Russel, *Cyber Blockades*, 100.

reached establishing Abkhazia as an independent region of Georgia. To keep the peace between South Ossetian separatists supported by Russia and Georgian troops, the Organization for Security and Cooperation in Europe (OSCE) facilitated an agreement of peacekeeping forces comprised of 500 Georgian, South Ossetian and Russian troops. Though officially an agreement was reached in both Abkhazia and South Ossetia, both conflicts went largely ignored and unresolved. Alison Lawlor Russel defines these conflicts as so-called "entropic conflicts that have the capability to leave to progressive disorder and chaos, if not resolved of managed effectively."[86] Even under the agreement reached with the help of OSCE, the South Ossetian capital of Tskhinvali fell victim to an increase in crime and corruption.

Essential background

The Georgian-Russian war was unique because it was the first time cyber attacks were employed together with a large scale military invasion in the context of warfare. Unlike the Estonian attacks, these cyber attacks clearly constituted part of what was an act of war. During the invasion of Georgia, Russia was successful in invading the three traditional battlefields: air, land, sea and using their cyber operations were able to invade Georgian cyberspace. The Russians showcased that cyber can be easily implemented and synchronized with other conventional methods of war enabling a more impactful form of warfare. While Estonia's internet is almost entirely independent and self-reliant, Georgia largely remains offline with transportation and power not powered by the internet. In 2008, at the time of the conflict, Georgia's internet penetration rate stood at 8 internet users for every 100 people, showing a lack of government and private sector investment in Georgian IT services and infrastructure.[87] The

[86] Russel, *Cyber Blockades,* 99.
[87] Russel, *Cyber Blockades,* 97.

internet infrastructure that does exist in Georgia is heavily dependent on Russia, with more than half of its telecommunications routes traveling through Russian territory, making Georgia extremely vulnerable, and allowing Russia the opportunity to easily manipulate Georgia's cyberspace. During the time of the conflict, Georgia was in the process of constructing a fiber optic cable between Georgia and Bulgaria to minimize Russia's influence over Georgia's IT infrastructure.[88] In addition, Georgia is an important transit point for major oil and gas reserves bordering the Caspian Sea, one of the only few in the region outside of Russian control, underlining its importance to the larger international market.

From 2003, after Georgia's Rose Revolution, relations between Russia and Georgia remained sour. From the Russian perspective the United States had had an invisible hand in the region to subvert Russia's influence in the region. In 2005, Georgia released a National Strategic Concept, which marked a change in identity shifting from a traditionally "South Caucasus identity" to identify with a "European Black Sea identity," as to align itself with the European Union and NATO. Tensions rose between Russia and Georgia with the detonation of shared electrical and gas pipelines located on the Russian side of the border. As a response, Russia imposed embargoes and many ethnic Georgians were deported from Russian, as the Georgian government also deported Russian spies.[89]

In Alison Lawlor Russel's book *Cyber Blockades,* she notes that Russia's support and recognition for the independence of South Ossetia and Abkhazia was a retaliatory move to counter the world community's recognition of Kosovo's independence on February 17th in 2008. Russia's decision to support South Ossetian and Abkhazian separatists and their rejection of

[88] Russel, 98.
[89] Russel, 100.

Kosovo's independence signals just another aspect of their continued hardline stance against NATO and the European Union's influence and the general culture of the West.

Tensions between Russia and Georgia continued into April of 2008, as a Georgian unarmed and unmanned aerial vehicle or UAV was shot down over the contested territory of Abkhazia. Following the incident, the Abkhazian government stated that Georgia had violated Abkhaz airspace claiming responsibility. In the following days, a video emerged which depicted that in fact a Russian Mikoyan MiG-29 had shot down the Georgian UAV, and as a response Russia sent peacekeeping forces into Abkhazia to maintain peace. In late May, Russia sent in additional troops to Abkhazia to repair a railway line, but Georgia took this as an act of aggression and as a part of a planned military intervention. In early July, violence in Abkhazia, ongoing since April, spread to South Ossetia and the rest of Georgia with both sides building up military forces and in turn violating the terms of ceasefire.[90]

The Attacks

On July 19, 2008, a distributed denial-of-service, or DDoS attack flooded and shut down Georgian servers and disabled the website of Georgian president, Mikheil Saakashvili, for 24 hours. Though no one has ever claimed responsibility for the attacks, it was found that the botnet command-and-control server,[91] also called a "bulletproof network" used in the attacks, was a so-called MachBot controller, which is often used by Russian bot herders.[92] In addition, the domain of the server[93] provided during the attack appeared to have falsified registration

[90] Russel, *Cyber Blockades,* 101.

[91] "A server that helps a fraudster to control a botnet and sends malicious commands to its members, regulate spyware, send payload, etc." ("Command and Control Server (C&C).")

[92] Russel, 101.

[93] "DNS servers located throughout the Internet are responsible for the translation of domain names into IP addresses. When a user types in a URL, a nearby DNS server will map the domain to an IP address or pass it to

information that could be traced to Russia. These July attacks became the petri dish for the subsequent attacks and invasion of Georgia.

The Georgian-Russian war started on August 7, 2008 when in response to Russian aggression, Georgian troops drove into the South Ossetian capital of Tskhinvali. As a response, Russian military forces also entered South Ossetia with airpower and infantry forces to supposedly protect Russian peacekeepers in the region. Meanwhile, 8,000 Russian troops lined the northern border between Georgia and Russia.[94] Later evidence was found that before Georgian troops had started their offensive on Tskhinvali, Russian troops had already been situating strategic military assets south of the Roki Tunnel, the official border between Georgia and Russia. It is clear that Georgia's seemingly absent 'aggression' did not warrant such a buildup of military forces on the Russian side. There seems to be a clear difference in military might, constituting these early stages of the crisis as a clear form of asymmetric warfare.

During the conventional military invasion, Russia and Georgia also engaged in information warfare on both sides to try to defeat the enemy by other means. Georgia, like Russia, shares a similar perspective of information warfare, viewing it as equally important to the actions on the battlefield. As Lawlor Russel writes, "they engaged in attempts to control the information available to the opposing side" to "justify their actions and gain approval in the international scene and generate or maintain support for their military both at home and abroad." [95] It is clear that Russia utilized this form of warfare as an extension of the physical battlefield to advance their agenda in the media, thereby having total control over the battlefield and

another DNS server. There is also a sort of 'mini DNS server' stored within Microsoft Windows operating systems, called the hosts file."("DNS (Domain Name System) Server.")

[94] Russel, 102.

[95] Russel, *Cyber Blockades,* 103.

information space. This also allowed Russia to control their response to the international community and what information it chose or did not chose to take at face value.

Cyberattacks were also utilized in conjunction with the ground and information assaults. Several websites were found defaced, among them the Georgian president, Ministry of Foreign Affairs and the National Bank of the Republic of Georgia. Posted to these websites were photos of Georgian president Mikhail Saakashvili and famous twentieth century dictators, including of Adolf Hitler. It was found that a hacking group based in South Ossetia claimed responsibility for the defacements.[96] Though the defacements resulted in an inconvenience for the Georgian government, they did not cause any significant damage and therefore could be regarded as a cyber riot or a form of online political protest.

The defacements were not nearly as damaging as the DDoS attacks which crippled the rest of Georgia. The DDoS attacks were launched at varying speeds, some of which, lasted approximately two hours and some lasting up until six hours.[97] Similar to the defacements the DDoS attacks were targeted at Georgian government websites, including the Parliament of the Republic of Georgia, the president of the Republic of Georgia, the government of the Autonomous Republic of Abkhazia, the Ministry of Education and Science of the Republic of Georgia, and the governmental website in charge of administering standardized tests for students. Furthermore, the websites of major communications and financial institutions were also targeted, including www.forum.ge, the largest forum based in Georgia, www.civil.ge, the largest English speaking Georgian news site, Associated Press, and other news sites.[98] Other notable websites that were attacked were www.kasparov.ru, the official webpage of the Russian opposition party

[96] Russel, *Cyber Blockades,* 103.

[97] Ibid.

[98] Russel, 104.

led by Garry Kasparov at the time. In the financial sector, the website of Georgia's largest commercial bank TBC was also attacked. In addition, the websites of the Supreme Court of Georgia, various embassies including of the United States and United Kingdom based in Tbilisi were also targeted.[99] From the pattern of targeted websites, it is clear that none of the websites were pro-Kremlin supported websites. All of the websites either supported Georgia, the European Union, Russian opposition parties and English speaking sites, pointing to the fact that whoever was responsible for the attacks had a agenda in mind supported by an anti-Western perspective --- like that of the Kremlin.

Implications

Over the course of the attacks, which lasted from August 8th to the 10th coinciding with the Russian offensive on the ground, 35 percent (over 100 internet networks) vanished from the Georgian cyberspace. Approximately 60 percent of the compromised internet networks were reported to be insecure at the time of the cyberattacks. The attacks originated from computers found all over the world, which in technological terms means that several botnets were used, a similar technique utilized in the Estonian cyber attacks of 2008. In Lawlor Russel's research, she notes that IT experts have noted that while the attacks on Georgia were meticulously planned beforehand in coordination with the the on-ground offensive, in Estonia, coordinated was only acknowledged later on after the second surge of attacks.[100]

Similar to how terrorists post videos and instructions on how to build a bomb, it was reported that Russian-language sites posted instructions on how to flood Georgian websites, including a list of vulnerable sites. Security experts have defined this form of spreading tutorials

[99] Russel, *Cyber Blockades*, 104.
[100] Russel, 105.

as a “cyber kill chain.” The primary two websites that were used in distributing these tutorials were xaker.ru and stopgeorgia.ru, using a parallel site called stopgeorgia.info. The stopgeorgia.ru website first became active in precise coordination with the on ground military offensive of South Ossetia on August 7th. The interesting nature of the structure of the website allowed it have a “bulletproof network” or a botnet command-and-control-server, which allowed users more online freedom.[101] If this website were traceable back to the Russian government then this would be another piece of evidence of how the Russian government manipulates the information space in its favor to have control over what it perceives as the truth, and in an effort to influence other actors to think in the same way. Publishing these websites publicly online is also an extension of Soviet strategy as well. The act of trying to recruit volunteer ‘soldiers’ to deface and disrupt these websites, if the publisher were the Russian government, displays a continuity between the recruitment of volunteer soldiers for the Red Army; this time only for Russia’s volunteer cyber army. The question still remains as to who uploaded this content to the public, and did the Russian government play a part or did fellow hackers post the material?

In remembering that most of Georgia’s telecommunications lines are routed through Russian territory, at the time of the attacks Georgian internet traffic was routed through Russia, subsequently denying Georgia the right to its own internet independence. Experts speculate that due to the fact that the lines shared by Georgia and Russia are under the control of the Russian Business Network (RBN), there is a possibility that the RBN could have been the perpetrator of the attacks.[102] It also happens to be that RBN employs a large number of state sanctioned hackers that work for the Russian government under anonymity. One of them, a Latvian-Russian Aleksey

[101] Russel, *Cyber Blockades,* 105.
[102] Russel, 106.

Belan, is currently on the FBI's most wanted list, unrelated to the Georgian attacks, but for conspiring in three massive data breaches of Yahoo spanning from 2013 up until its discovery in 2016.

It is clear that by coordinating the cyber attacks and the offensive on the ground in the invasion of Georgia, was effective in limiting Georgia's communication between the people and the government and the government and the international community. A similar effect was seen in the aftermath of the cyberattacks on Estonia. While the invasion of South Ossetia was a clear violation of Georgia's territorial sovereignty, the cyber attacks in coordination with the defacements can be considered a violation of Georgia's internet sovereignty. The largest negative effect of the cyber attacks was the fact that the people of Georgia were unable to access official government websites and media reporting of the waging war in South Ossetia, while at the same time the Georgian government was unable to communicate with the rest of the world community, [103] which destabilized the governance of the state. In addition, on August 9, the National Bank of Georgia was attacked by cyber attacks terminating all online banking services, which lasted a full 10 days.[104] Due to the nature of military invasions, during which time economic damages are difficult measure, in Georgia it was ever more difficult to determine the economic losses due to the incorporation of information and cyber warfare.[105]

International response to attacks

RUSSIA

The Russian Embassy based in London, released a statement stating they had no knowledge of the attacks on Georgia both military and cyber, instead defining the offensive in

[103] Russel, *Cyber Blockades,* 107.
[104] Russel, 108.
[105] Ibid.

South Ossetia as a supposed “peace enforcement” operation. Meanwhile, the Kremlin also released a statement that said it had no involvement in the attacks on Georgia.[106] This response from both the Russian Embassy and the Russian government came as no surprise, especially following the attacks on Estonia from a year before where the Russian government also had adamantly claimed no involvement.

IT experts on the other hand have asserted that though there is no conclusive evidence of the Russian government’s connection to the attacks, there appears to be some proof that the Russian Business Network could have had a hand in the attacks. They do however assert that the RBN may not have administered the attacks but instead may have accommodated the “bulletproof networks” in a coordinated effort.[107] Though there is not enough sufficient evidence to prove that the Russian government had a direct involvement in the attacks, the Kremlin did at least tolerate and support the attacks, considering the attacks were spent in a clear side-by-side planning with the Russian military forces invading South Ossetia.

Project Grey Goose, now formally called GreyLogic, was launched in 2008 as a response to the cyber attacks on Georgia to investigate how the cyber war was waged in Georgia and if the Russian government played any involvement in the attacks. According to Project Grey Goose, the cyber attacks appeared to possibly have been facilitated by an organization observing different phases of the attacks.[108] Lawlor writes that the first stage involved “encouraging activists to become involved in the cyber war against Georgia,” secondly “publishing a list of accessible targets,” thirdly “selecting malware for us in the attacks,” and finally “launching the

[106] Russel, 109.
[107] Ibid.
[108] Lewis, “Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare.”

cyber attacks, and evaluating the results,"[109] all of which adds to cyber warfare. After Project Grey Goose completed its investigation, they released their findings stating:

> We assess with high confidence that the Russian government will likely continue its practice of distancing itself from the Russian nationalistic hacker community thus gaining deniability while passively supporting and enjoying the strategic benefits of their actions.[110]

The findings Project Grey Goose presents are compelling because surrounding the literature discussing Russia's connection to the hacker community, often times scholars and researchers have not wanted to definitively assert that a relationship exists, due to the fact that the sparse evidence that is available is not enough to draw a definitive conclusion. On the other hand, Project Grey Goose suggests a different option in which there may have previously existed a relationship, but in the process of severing those ties the Russian government chooses not condemn the actions of these individuals, but instead provide them with a space to function without any circumstances, therefore tolerating their presence and maintaining their own desired level of plausible deniability. It's a "win-win" situation in which both sides benefit and therefore both rely on one another for mutual protection.

THE EUROPEAN UNION

As mentioned earlier, Georgia is not a member state of the European Union, instead its relationship with the European Union is facilitated by the Partnership and Cooperation Agreement (PCA). President Sarkozy, at the time, the president of the European Union, brokered a ceasefire on August 12, 2008.[111] When Russia refused to withdraw its troops, as a part of the terms of the ceasefire, the E.U. decided upon condemning Russia's recognition and support for

[109] Russel, *Cyber Blockades,* 110.
[110] Lewis, 111.
[111] Russel, 112.

the independence of South Ossetia and Abkhazia, while also not renewing the partnership between Europe and Russia until troops were withdrawn.[112] The lack of unity between member states meant that the European Union had lost an opportunity to formulate a definitive response to the war, which would have more effective in countering Russia's aggression. The European Union receives one third of its oil from Russia as well as 40 percent of its natural gas, therefore any action that the E.U. decided to take, would have to have been seriously considered noting their energy dependency on Russia. Though the European Union struggled coming to a consensus, member states were able to provide financial aid to Georgia. The E.U. added 120 million euros in post-crisis assistance to its usual 42 million euros, and in addition individual E.U. member states provided 8.4 million euros for additional support.[113]

NATO

Though Georgia was not a member state, at the time NATO had opened up discussions on admitting Georgia. Georgia remains a NATO partner, having participated in NATO missions in Afghanistan in the past. NATO, like the E.U., was very concerned about Russia's actions and invasion of South Ossetia and Abkhazia, highlighting the "disproportionate use of force."[114] NATO also sent in experts to assess damage specifically to civil infrastructure, and stressed its recognition of Georgia's sovereignty "within its internationally recognized borders," including South Ossetia and Abkhazia as Georgian territory. Jaap de Hoop Scheffer, the NATO secretary general at the time, expressed his criticism for how "vaguely" the E.U. had handled the crisis,

[112] Russel, *Cyber Blockades,* 112.
[113] Russel, 113.
[114] Russel, 115.

nothing that the E.U. had provided too many "concessions to Russia and not opposing Russian violation of the agreement."[115]

Though Lawlor Russel presents a very precise and accurate retelling of the cyber attacks and invasion of Georgia in 2008, there are some important factors missing from the way she chooses to discuss Russia's approach to cyber and information warfare. In Lawlor Russel's retelling she seems to assume that information warfare and cyber warfare are separate entities, the position often taken by the West, as a result her account of the Georgian war is largely from the perspective of the West. I believe she does not stress enough how groundbreaking the strategic implementation of cyber, in conjunction with on ground operations, over the course of the war, was vital to the actualization and development of Russian military doctrine in 2010 and then again in 2014. It is important to stress, once again, that Russia approaches both forms of warfare as integrated systems, emphasizing Russia's approach as an entirely different from the West. Therefore this is a new way of waging warfare for the West but it is a strategy associated with asymmetric and hybrid warfare familiar to Russia that has been employed in the past, which only recently has become more visible in the attacks on Estonia, Georgia and Ukraine.

Part 3: The Ukrainian War (2014)

Essential Background

Over the course of the past four years, war has continued to disrupt the civil society of Ukraine, even as the media has moved on to cover the next attractive crisis. Often times, it is forgotten in the information glut that the crisis in Ukraine started over a supposed trade

[115] Russel, 116.

agreement gone wrong. Ukrainian President Viktor Yanukovych had promised that he would sign a trade agreement with the European Union, which would have been a monumental achievement in an effort to solidify ties with the E.U. Instead President Yanukovych adjourned talks with the E.U. due to the strong dissent of the Kremlin, which had had a history of opposing Ukraine's interest in joining and forming a closer relationship with the E.U. On November 21, 2013, thousands upon thousands of protestors took to the streets in reaction to the presidential decision, emphasizing the increasing divide between the pro-European west and those in support of Yanukovych's pro-Kremlin government.[116]

History of the conflict: The Annexation of Crimea

On February 20, 2014, after months of low level violence, a violent gunfight erupted in Maidan Square (or independence square in Kiev) leaving dozens dead. This incident sparked reactions from the protesters who claimed that government snipers were planted and instructed to kill protestors, whereas the government claimed that opposition leaders were to blame for provoking the violence. Just two days later on February 22, Yanukovych's guards abandoned their posts at the president's compound and Yanukovych conveniently fled. In the meantime, the former Prime Minister of Ukraine, Yulia Tymoshenko, jailed since 2011 after a politically driven trial, was also released and consequently addressed the pro-Western protesters in Maidan Square as an attempt to rally support, confidence and hope. Similar to protests during the Arab Spring in Cairo, and even Occupy Wall Street in New York City, protestors occupied Maidan Square day and night as a symbolic protest to spark a reaction from the world community and the Russian backed government.[117]

[116] CNN, "Ukraine."

[117] Ibid.

Only a week later on March 1st, the Russian parliament confirmed President Putin's appeal to deploy Russian military forces into Crimea, a region of southern Ukraine that has a large population of ethnic Russians and politically pro-Kremlin. After the confirmation of the Russian parliament, thousands of so-called 'little green men' in unmarked uniforms invaded the peninsula of Crimea bordering Russia. In only two weeks, Russia had successfully annexed Crimea in an extremely controversial referendum heavily opposed by many in western Ukraine and the international community. Subsequently, on April 15, the Kiev government launched its first military operation against the pro-Russian rebels who had seized government buildings across eastern Ukraine, and a month later separatists in Donetsk and Luhansk already had declared independence following unrecognized referendums.[118]

On May 25th, Petro Poroshenko, a candy magnate and one of Ukraine's richest men, was elected into office, meanwhile reports emerged that pro-Russian separatists in eastern Ukraine had engaged in voter suppression to change the results of the election. After months of violence, the same deal which former President Yanukovych had adjourned abruptly before fleeing due to backlash, on June 27th President Poroshenko successfully signed the E.U. Association Agreement, sending a message to Russia that Ukraine was still seeking to maintain a relationship with the European Union. Over a month later, on June 17th, the commercial airliner Malaysia Airlines Flight 17 went down above rebel-held territory in eastern Ukraine and all 298 people on board died. It was later discovered that the airliner was shot down by a surface-to-air missile based in the rebel-controlled region of eastern Ukraine near Donbass, once again sparking more tensions between Ukraine and Russia.[119]

[118] CNN, "Ukraine."

[119] Ibid.

Months later on September 20th, a complete ceasefire was finally reached between Ukraine and the pro-Russian separatists, which stated that both sides must back down militarily, while Russian caravans of trucks were discovered crossing the Russian-Ukraine border supposedly for humanitarian aid. On November 12th, a NATO commander revealed that in fact Russia had not retrieved from the Ukrainian border, instead had continued providing the rebels with the means to continue to wage the conflict, violating the September ceasefire — which Moscow also denied. This fact highlights the asymmetric nature of the Ukrainian war, as well as another point on the continuum between Soviet and Russian military strategie.

Starting with the new year, on January 22, 2015, the Donetsk International Airport in eastern Ukraine finally fell to the separatist rebels, and a few days later, President Poroshenko called for the International Criminal Court (ICC) to investigate "crimes against humanity" due to the increasing dire situation in eastern Ukraine. A month later, Angela Merkel and Francois Hollande advocated for another ceasefire agreement after the United States proposed supplying the Kiev government with lethal aid. After the ceasefire went into affect on February 12th, Ukraine's National Defense and Security Council reported that there had already been instances of 300 violations of the ceasefire by February 20th. On June 22, seeing that the ceasefire was not productive in alleviating the conflict, foreign ministers of the E.U collectively imposed sanctions against Russian in response to Russia's military aggression over the past months, to which the Russian government responded calling them "unfounded and illegal."[120]

Nearly a year later, on March 3rd, 2016, the United Nations released its own statement expressing concern over the drawn-out deadlock affecting millions in the eastern half of Ukraine.

[120] CNN, "Ukraine."

Since April 2015, approximately 9,500 people had been killed in the ongoing conflict while 22,100 more injured, according to the UN. On August 5th, the Office of the UN High Commissioner for Human Rights released factual data depicting a rise in civilian casualties, specifically in eastern Ukraine. The agency found that 69 civilians were found dead in June --- the highest death toll since August 2015. Later in December, the Ukrainian military conducted missile launches near the Crimean border, to which Russia immediately countered stating that it was in violation of international agreements. Russia viewed the missile launches as a threat to their border security recognizing Crimea as Russian territory after the annexation. Meanwhile, the international community recognized the missile tests as lawful under existing international agreements due to recognizing the territorial sovereignty of Crimea and eastern Ukraine as Ukrainian sovereignty.[121]

"Operation Armageddon"

Published in 2015, midst the attacks against Ukraine, Lookinggglass Cyber Threat Intelligence Group, proposed research on Russian cyber warfare targeted against Ukraine titled *Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare.* The research speculates that the so-called "Operation Armageddon" (originally misspelled as "Armagedon") had been already active since 2013, siting clear prior planning on the part of the Russian government. The goal of using cyber to achieve Russia's objectives was to "provide a military advantage to Russian leadership by targeting Ukrainian government, law enforcement, and military officials in order to steal information that can provide insight into near term Ukrainian intentions and plans."[122] According to Lookingglass, the attacks started in tandem

[121] CNN, "Ukraine."

[122] Lewis, "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare," 3.

with Ukraine's decision to sign the European Union Association Agreement on June 27th. Though that Russia may have already been preparing for this attacks as early as 2012 in preparation for the possibility that Ukraine would sign the agreement. The earliest timestamp of malware stated the date June 26, 2013 after which more timestamps were found also correlating with the 10th Yalta Annual Meeting between August 12 and September 16th of 2013. The annual meeting attended by 250 leaders from 20 countries was meant to draw attention to the future of Ukraine, which may have been the "catalyst" for Russia to implement its cyber operations due to the threat of Ukraine closing ties with the European Union. Lookingglass does note that the attacks increased in the aftermath of Yanukovych fleeing his compound in on February 22, 2014 and the interim government announcing the beginning of an "anti-terrorist operation" against the pro-Russian separatists. From that point forward the attacks became ceaseless, again in coordination with Russia's military actions on the ground, similar to Russia's military strategy in the Georgian-Russian war, from which Russia definitely learned was an effective strategy for obtaining information and intelligence, and therefore gaining leverage.

Lookingglass found that according to statements made by the Security Service of Ukraine (SBU), the attacks were administered by the 16th (formerly known as the Federal Agency of Government Communications and Information) and 18th Centers of the Russian FSB. As opposed to the attacks in Georgia, where it was inconclusive if the FSB was involved in administering the attacks, this was the first time throughout all three case studies that the Russian attacks could not only be traced back to Russia but traced to the Russian government, siting that the Russian government was actively implementing cyber warfare and espionage as a part of their military strategy in the Ukrainian war.[123]

In the section of their research focused around the tactics used in Operation Armageddon, Lookingglass reported a pattern in the attacks starting with the dispersal of targeted spear-phishing emails a strategy not used in either Estonia or Georgia, siting a new form of attack developed by Russia. These emails arrived in inboxes disguised as documents originating from Ukrainian officials, often directly stolen from the very officials, to convince the user to open the infected content. Some of the so-called "payloads" came disguised also as updates for Adobe Flash Player, Internet Explorer or Google Chrome. In addition, some payloads over the course of the operation were forms of RAT, a type of malware that has the ability to control a system through a remote network connection. In the case of Ukraine, specifically a Remote Manipulator System was used, which according to Lookingglass is a common RAT used by Russian hacking forums, and has been classified by the AntiVirus industry as malicious. The way these RATs were used to obtain information during the Ukrainian-Russian war were then able to be used later as 'lures,' in a sense building on top of one another. The conflict on the ground together with the momentum of the cyber attacks and RATs may have been the reason why the attacks last over the course of many years, rather than just a few weeks or days, therefore proving to be more effective as the attacks in Estonia and Georgia. It is clear based off of Lookingglass' research that the attacks on Ukraine were purely for Russia to have a military advantage over the Ukrainian forces, gaining access to information and intelligence on Ukrainian strategy.[124]

[123] Lewis, "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare, 6."
[124] Lewis, 7.

The Ukrainian war demonstrated, more so than Estonia and Georgia, that cyber warfare and the ‘little green men’ are linked as a part of Clausewitz’ approach to consolidating all aspects of the state. Ukraine displayed the level in which the Russian military was able to dominate all of Ukraine’s domains including land, sea, air, space by having foremost control of the information space. While in Estonia, cyber was used to disrupt internet activity, in Georgia this strategy was used side-by-side with the military invasion, ultimately all of these strategies culminated in using cyber warfare to gain intelligence and leverage over on ground Ukrainian military forces. This leveraging of information is an indicator of the direction in which Russian military strategy will take moving forward. Rather than implement cyber when necessary, as case-by-case, like the United States, Ukraine is evidence of the fact that Russia is aiming for cyber warfare to have an integrated role in how their military functions both in the cyberspace and in also in conventional terms.

Conclusion

I first set forth to examine the effect of Russian cyber warfare on the Baltic states, as I had lived and worked recently in Latvia, the country of my ancestors. After the 2016 U.S. presidential elections, I quickly realized Russia's targeted use of cyber warfare was not specific to the Baltic region, but affected the whole post-Soviet bloc. In studying the 2008 cyber attacks on Estonia, I found that Georgia and Ukraine shared very similar experiences, and therefore determined to concentrate on Russia's offensive use of cyber for the purpose of maintaining its sphere of influence in the area of the former Soviet bloc. While I had initially intended to study Russia's manipulation of proxy actors as a volunteer "cyber army," I became fascinated by the influence of Soviet military doctrine on Russia's current use of cyber warfare.

The goal of this paper was to examine how Russian military strategy has been able to include cyber attacks into the umbrella term of information warfare. The continuity between Russian and Soviet military strategy can be seen by studying three components of this strategy: the mobilization of the state, the offense-defense balance (or imbalance, in the case of Russia), and the role of Soviet partisan warfare as the basis for later use of asymmetric and hybrid warfare.

In the Soviet era, the mobilization of the state was meant to protect the Revolution within the confines of the Union, and later to prepare the state for war. One can say that mobilization is now embodied in the information space itself. By manipulating cyber space to have it take control of the functions, and, most importantly, the discourse of other sectors of governance, it has taken on the role of mobilization. The role of the information space is evident in the three cases of Estonia, Georgia and Ukraine, in which the inflicted cyber attacks all had an effect on the communications in the three countries during the time of the attacks, affecting how the governments could communicate with their people and with the outside world.

Similarly, the offense-defense balance has played a very significant role in the development of Soviet military strategy. The Soviet regime had difficulty actualizing this balance in its doctrine before the onset of World War II. As a result, what was supposed to be a balance became an imbalance favoring the offense over the defense. The emphasis on offense both aided and inhibited the creation of Soviet military strategy. One way in which it aided Russian military strategy was that it facilitated the inclusion of cyber into the total doctrine. Russia has embraced an almost entirely offensive military strategy well into the 21st century, a fact which is evident in the three case studies outlined in this project.

Lastly, partisan warfare, originally inspired by the peasant and proletarian uprisings during the Soviet era, has evolved into the asymmetric and hybrid forms of warfare of today. This can be traced from Soviet military history, beginning as far back as World War I, and continuing throughout World War II, a strategy often due to limited resources and supplies. Now in modern strategy, this method of waging war and conflict has continued to develop, partly due to the fact that asymmetric and hybrid warfare work well hand-in-hand with cyber, which favors the offensive. The conflicts described in all three case studies can be categorized either as asymmetric or as hybrid warfare, or as both – supporting the conclusion that Russia's use of cyber warfare is an extension of asymmetric and hybrid methods.

In the future, I hope to expand upon this project and to study Russia's alleged use of a volunteer cyber army to carry out its form of cyber warfare, which, if proven to be true, would display yet another point of continuity between the Soviet and Russian military doctrines. In researching Russia's form of cyber warfare, I have found the literature to be very vague and non-specific in identifying the role of the Russian government as an actor in international cyber aggression.

I believe that it is high time for Russia's use of cyber warfare to be fully disclosed to the Russian people and to the world community. My personal – not academic – goal when beginning this project was to do just that. In the process, I became overwhelmed by the plethora of literature on the topic, and hindered by the fact that I am neither a coder nor a Russian speaker. I believe that Russia's use of cyber warfare is important, not because Russian is the only actor that engages in cyber warfare, but because Russia's use of cyber warfare is so opaque. Its methods allow the Russian government to act under the radar, knowing they will receive little or no condemnation, or at least scrutiny, by the international community – creating an efficient form of aggression that in my eyes is quite dangerous for the United States and the world.

Bibliography

Ashmore, MAJ William C. “Impact of Alleged Russian Cyber Attacks.” *School of Advanced Military Studies United States Army Command and General Staff College* 11 (May 21, 2009): 58.

Bērziņš, Jānis. “Russia’s New Generation Warfare in Ukraine: Implications for Latvian Defense Policy.” *National Defense Academy of Latvia Center for Security and Strategic Research* 2 (April 2014): 1–13.

CNN, Nick Thompson. “Ukraine: Everything You Need to Know about How We Got Here.” CNN. Accessed March 28, 2019. https://edition.cnn.com/2015/02/10/europe/ukraine-war-how-we-got-here/index.html.

“Command and Control Server (C&C).” Accessed April 30, 2019. https://encyclopedia.kaspersky.com/glossary/command-and-control-server-cc/.

Dexter, Byron. “Clausewitz and Soviet Strategy.” *Foreign Affairs* 29, no. 1 (1950): 41–55. https://doi.org/10.2307/20030813.

“DNS (Domain Name System) Server.” Accessed April 30, 2019. https://encyclopedia.kaspersky.com/glossary/dns-domain-name-system-server/.

Galeotti, Mark. “Hybrid, Ambiguous, and Non-Linear? How New Is Russia’s ‘New Way of War’?” *Small Wars & Insurgencies* 27, no. 2 (March 3, 2016): 282–301. https://doi.org/10.1080/09592318.2015.1129170.

Geltzer, Joshua A. “Stop Calling Them ‘Russian Troll Farms.’” CNN. Accessed April 27, 2019. https://www.cnn.com/2018/08/17/opinions/stop-calling-russian-operatives-troll-farms-geltzer/index.html.

Grassegger, Hannes, and Mikael Krogerus. “Weaken From Within.” *New Republic* 248, no. 12 (December 2017): 16–23.

Gvosdev, Nikolas K. “The Bear Goes Digital:” In *Cyberspace and National Security*, edited by DEREK S. REVERON, 173–90. Threats, Opportunities, and Power in a Virtual World. Georgetown University Press, 2012. http://www.jstor.org/stable/j.ctt2tt6rz.15.

Herzog, Stephen. “Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digitial Insecurity.” *Georgetown Journal of International Affairs* 18, no. 3 (Fall 2017): 67–78.

Kampmark, Binoy. “Cyber Warfare Between Estonia and Russia.” *Contemporary Review* 289, no. 1686 (Autum 2007): 288–93.

Kasparov, G. K., and Mig Greengard. *Winter Is Coming: Why Vladimir Putin and the Enemies of the Free World Must Be Stopped*. First edition. New York: PublicAffairs, 2015.

Laasme, Haley. “Estonia: Cyber Window into the Future of NATO.” *Joint Force Quarterly*, 4, no. 63 (2011): 58–63.

“Leon Trotsky | Biography, Books, Assassination, & Facts.” Encyclopedia Britannica. Accessed April 26, 2019. https://www.britannica.com/biography/Leon-Trotsky.

Lewis, Jason. “Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare.” LookingGlass Cyber Threat Intelligence Group, April 28, 2015.

“Malicious Software.” Accessed April 18, 2019. http://www.seas.ucla.edu/security/malware.html.

Maness, Ryan C., and Brandon Valeriano. “The Impact of Cyber Conflict on International Interactions.” *Armed Forces & Society* 42, no. 2 (April 2016): 301–23. https://doi.org/10.1177/0095327X15572997.

Michael Connell, and Sarah Vogler. “Russia’s Approach to Cyber Warfare,” March 2017, 1–29.

Rice, Condoleezza, Gordon A. Craig, and Felix Gilbert. “The Making of Soviet Strategy.” In *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, edited by Peter Paret, 648–76. Princeton University Press, 1986. https://www.jstor.org/stable/j.ctv8xnhvw.26.

Russel, Alison Lawlor. *Cyber Blockades*. Georgetown: Georgetown University Press, 2014. https://www.jstor.org/stable/j.ctt9qdsfj.10.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. Second edition. New York: PublicAffairs, 2017.

Shackleford, Scott J. “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law.” *Berkeley Journal of International Law* 27, no. 1 (2009): 203–10.

Slayton, Rebecca. “What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.” *International Security* 41, no. 3 (January 2017): 72–109. https://doi.org/10.1162/ISEC_a_00267.

Stapleton-Gray, Ross, and William Woodcock. “National Internet Defense---Small States on the Skirmish Line.” *Communications of the ACM* 54, no. 3 (March 1, 2011): 50. https://doi.org/10.1145/1897852.1897869.

“The Military Doctrine of the Russian Federation (2010).” Russian Federation presidential edict, February 5, 2010. https://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

“The Military Doctrine of the Russian Federation (2014).” Russian Federation presidential edict, 2014. https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf.

Wirtz, James. “Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy.” In *Cyber War in Perspective: Russian Aggression Against Ukraine*, Kenneth Geers., 29–37. Tallinn: NATO CCD COE Publications, 2015. https://pdfs.semanticscholar.org/7ccc/d4a0c3861ebf6f49dc32c8246248a97af4fd.pdf?_ga=2.172108010.818330443.1556379400-337160625.1556379400.