Analyzing How Russia Uses Cyberattacks to Project Geopolitical Power Through the Lens of Just War Theory

A Research Paper

John McFarland

CYBERCRIMINOLOGY MAY 10TH 2017

It is the goal of every regional power to expand its influence and become a world power. Since the fall of the Soviet Union, the Russian Federation has used every tool in its arsenal to achieve that goal. In the modern era, that endeavor is more difficult thanks to the North Atlantic Treaty Organization (NATO), the European Union, and the United Nations (UN). For a country to justify traditional warfare, it needs to follow the Law of Armed Conflict (LOAC). Without a valid cause, various countries may rally around the victims of aggression and punish the aggressor. This uneasy agreement between countries has been the foundation of international politics since the end of World War II, but with these laws so narrowly interpreted advances in technology have allowed new theaters of warfare to open. To circumvent these laws that have restricted Russian geopolitical power, Russia has expanded its arsenal to include cyberattacks that slip beneath the accepted definition of cyberwar. Over the last decade, Russia has engaged in a series of cyberattacks against neighboring countries as a method of exerting geopolitical power, and to reassert itself as a world power. Looking at two cases where Russian cyberintrusion achieved geopolitical goals, it needs to be asked if these attacks were enough to be considered cyberwarfare, and if so, did they violate the LOAC's determination of Just War?

1. What is Just War?

"Traditional Warfare is guided by just war theory, which provides guidance to countries on legitimate justifications to go to war (jus ad bellum), and what constitutes as ethical conduct in war (jus in bello). " (Maras, pg. 396)

From the earliest recorded philosophy, humanity has considered jus ad bellum. As humanity sought inner peace, it needed to justify the violent world it existed in. The earliest example of just war is found in the Indian epic Mahabharata. The Mahabharata describes a code of conduct for war that was agreed upon by two warring sides (Thapar, pg.1830). These rules

sought to ensure that a war was righteous or just. The philosophical questions were rooted in a desire to retain 'goodness', and to ensure that war only ever went as far as it needed to.

The effort scholars and lawmakers make to regulate warfare continues into the modern day. After the horrors of World War II, the world wanted to establish a set of regulations to ensure that it never experienced the same level of suffering. In an effort to limit the effects of armed conflict, the international community came together at the First Geneva Convention of 1949 to revise the existing three Geneva convention treaties, and to add a fourth. The Geneva Convention is one of the foundations for International Humanitarian law that codifies the acceptable conduct of war, which lays the path for Just War Theory.

The characteristics of a Just War are heavily debated. Looking at the four theorists examined in Christopher Toner's paper "The Logical Structure of Just War Theory", the only agreed upon characteristics are just cause, and right intention (Toner, pg.83). The most extensive list of characteristics is by James Turner Johnson. Johnson lists just cause, right intention, right authority, proportionality of ends, last resort, reasonable hope of success, and aim of peace as the criteria for a Just War (Toner, 82). Using Johnson's metric allows for closer examination of Russia's cyberattacks that may be more forgiving. (Zehr, pg.191)

2. Geopolitics and Power projection

The struggle between competing nations is as old as humanity. But that struggle has changed drastically since the establishment of Mutually Assured Destruction (MAD). Before MAD, a powerful country could mobilize its military, and conquer their competitors without fear of repercussion. But after MAD was established, nuclear weapons, intercontinental ballistic missiles (ICBMs), and multiple independently targetable reentry vehicles (MIRVs) ensured that

any direct attack would be met with a nuclear response. This situation forced a stalemate between competing powers that resulted in the Cold war. The Cold War saw America and Russia compete to collect countries for their respective hegemonies and ideologies. America has led the liberal global order founded on capitalism and democracy, while the Soviet Union worked to undermine them with the goal of spreading communism and establishing its own hegemony over Europe.

Traditionally power is projected in two ways; military force, and economic force. Considered geopolitically, America has the advantage of using the oceans as natural barriers. Bradly S. Klein describes American strategic culture with "This is the strategic culture of a country that always goes to war 'over there', overseas. It is a country that has remained relatively isolated from world affairs because of its geography." (Klein, pg.136) At the end of WWII, America's manufacturing industry was untouched while the Soviets were still recovering from German invasion. This allowed America to reach out to other countries destroyed in the war and lend them money, sell them supplies, and rebuild them. This economic projection helped bring Europe into the fold. As America became more powerful, the Soviets became more cunning. While America mobilized its massive economy into military research, the Soviets focused on its spy tradecraft and subterfuge. While information in America was free and unregulated, a totalitarian Soviet Union was immune to propaganda. Leaning on the skills they learned during domestic subjugation, the Soviets learned how to spread propaganda overseas. The Soviets used those tools to take advantage of American political divisions to drive a wedge between the American government and its people.

In places where the Soviets were successful in spreading communism, America would either continue to project economic power by funding opposing factions to disrupt communist regimes, or they would project military power and overthrow them. While America was not always

successful, they made every Soviet victory cost as much as possible. America outspent the Soviets, forcing them to spread themselves too thin by keeping them constantly committed to defending their own borders. This prevented them from consistently being able to apply pressure on the United States.

The Soviet Union's economy could not keep pace with America, and it limited their ability to project power. On December 26th, 1991, the Soviet Union dissolved. The remnants of its political power split between its client states, and its spiritual successor, the Russian Federation, was born. To analyze Russia's geopolitical goals, it is necessary to understand the environment they exist in. As Russia struggled to rebuild its economy, the former Soviet bloc states rushed towards NATO for safety from their former occupiers. America took this opportunity to expand its hegemony right to Russia's borders. Russia considers this expansion a violation of an agreement made during the end of the Cold War.

Now twenty-six years after the dissolution of the cold war, the geopolitical climate has changed. With the creation of the internet and the birth of the information age, a new way to project power emerged. This offered Russia a few new ways to project power. First, by utilizing connected critical infrastructure, Russia could cause damage to an adversary's critical infrastructure without mobilizing troops. Second, Russia now has the ability to manipulate information in enemy territory without fielding agents. Instead, Russia legally allows its citizens to participate in cybercrimes against other nations. This gives Russia deniability during international conflict, while also giving them the ability to augment their state efforts during cyberattacks.

3. Russian Cyberaggression through the lens of Just War theory.

Tensions between Russia and Estonia began as soon as the cold war ended. Estonian independence saw domestic celebration of Estonian acts of resistance against Soviet occupation. As former Soviet bloc states gained independence, they looked towards the west for protection from their former occupiers. Happy to oblige, NATO began talks with Estonia and others in 2002 to join NATO, and finalized those talks on March 29th, 2004 when Estonia joined NATO as an official member. This caused tensions with Russia who saw this as the west encroaching on their territory.

Russian cyberaggression against Estonia began on April 26th, 2007 with a series of Distributed Denial of Service(DDOS) attacks against the nation's digital infrastructure. These attacks followed the Estonian government's decision to relocate a Soviet Era memorial to fallen soldiers called the "Unknown Soldier". According to Kertu Ruus, the statue was "A symbol of foreign occupation, it was never popular: Estonians dubbed it 'Unknown Rapist'. It was a gathering place for Red Army soldiers and their compatriots in the 400,000-strong minority community of ethnic Russians, sometimes for boisterous occasions celebrating Soviet holidays" (Ruus, pg.21). This decision angered Russia, who claimed that removal of the statue was disrespectful to the Soviet soldiers who died defending Estonia, and could lead to discord between the two nations. While Russia denies that it led the attacks, Russian language web forums consistently incited protestors in Estonia to action, and provided direction and resources for cybercriminals to attack Estonian infrastructure. "In retrospect, Estonia's Ministry of Defense now can reconstruct the assault as a two-phase offensive. For the first few days, the attackers – 'Hacktivists' – were engaged in amateurish psychological warfare with propagandistic goals… in the second phase in

which cyberattack specialists joined the fray and escalated the attacks into a full-scale campaign." (Ruus, pg.21)

As the attacks continued, Estonia mounted a defense. Considering the nature of a botnet, they looked for ways to slow the amount of traffic trying to access critical infrastructure. Once Estonian officials identified the attacking computer's IP addresses, they requested they be blocked by DNS administrators. This strategy gave the Estonian defense the ability to bring systems back online, and to start the road to recovery. Estonia tried to hold Russia accountable because some of the attacking systems were traced back to Russian President Vladimir Putin's administration, but Russia denied it had a role in the attacks. According to Russia any computer related to the Russian government must have been a zombie system in a botnet. When Estonia asked for Russia's cooperation with investigating further to prove or deny these claims, Russia declined to help.

Experts agree that the attack on Estonia were largely symbolic, it represents a much larger political principle. If you go against Russia, Russia will punish you. With traditional warfare, potentially triggering Article V of the NATO would mitigate this type of behavior- but in cyberspace, it is still debated if cyberattacks are an act of war. This was the first major instance of Russia using cyberattacks to project geopolitical power, but were they justified? Looking at Johnson's criteria for Just War may provide an answer.

Did Russia have just cause? Article2(4) and Article 51 of the UN charter suggest no. Article 2(4) states that: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." This is supplemented by Article

51 which states: “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.” (UN Charter, Article 2 & 51). Because no armed attack occurred against Russia, they did not have the just cause of defending themselves under international law. However, Russia views cultural attacks as existential attacks, and sees this action as defending its cultural heritage. While this reason does not justify the attack, it does make sense when considering Russia’s geopolitical goals. It is possible that Russia saw this action as a way to ensure peace by using cyberattacks to influence Estonia instead of military force, but the indiscriminate nature of the attack caused a disruption to peace itself. If true, that would indicate that Russia had the right intention. If they had the right intention, did Russia have the right authority? From the Russian perspective, they did. The importance Russia puts on Soviet culture as an existential part of Russian security provides their sovereign with the justification to act to ensure it. Did Russia consider the proportionality of ends? “Proportionality involves considering all the evil resulting from a war, and weighing it against the good that will occur or the harm that will be avoided.” (Brown, pg. 172) This is undetermined. While there is no way to know how Russia concluded what it did, Russia’s decision to use cyberattacks instead of military force may reflect a desire to minimize damage while projecting force. However, the indiscriminate nature of the cyberattack and its effects on the civilian population suggest otherwise.

The Russia cyberattacks against Estonia were not a last resort. Russia was never put into a position where it needed to act, and though they contend that dismissal of Soviet culture is an existential threat, they were not militarily or economically threatened. Therefore, they were not pressured to act. It is unclear if Russia believed this specific incident was going to be successful. Without taking credit for the attacks, there is no way to determine if they felt this was a success or a failure. The only metric to consider is if they engaged in similar actions afterwards, and looking at continued Russian cyberaggression suggests that it was a success. It is more likely that Russia used this attack to measure the effectiveness of cyberattacks. When considering if there was an aim for peace it depends on how peace is defined. There was no physical threat to peace to begin with, but because Russia views dismissal of Soviet culture as an existential threat to its peace, the position can be taken that Russia saw cyberattacks on Estonia as a way to pressure them into reversing their decision to remove the Soviet monument, which would be a return to peace.

Determining if Russia's cyberattack on Estonia was just depends on how a nation should respond to existential threats. Looking at the individual criteria for a Just War as described by Johnson, Russia's actions seem reasonable. They felt their power was threatened, and acted on it. In addition, the minimal damage caused makes this more of a cyberprotest than cyberwarfare. However, accepting that justification in context makes Russia's actions a lot less reasonable. Russia was under no physical threat from Estonia, and Russia's desire to retain its influence came at the expense of a nations sovereign rights. Since Estonia was already looking outward for protection from Russia, actions like this only deepen the divide between those two nations.

Russian cyberinterference did not stop with Estonia. In August 2008, Russia conducted cyber operations against Georgia. Unlike Estonia, these cyberattacks were coordinated with traditional military operations. Georgia was dealing was an insurrection from the South Ossetians, a semi-autonomous region in the South Caucuses. During the conflict, Russian peacekeepers were killed during the shelling of an Ossetian town, and the Russians used that as an opportunity to get involved.

The conflict with the Ossetians goes back to 1989. The Ossetians felt that their culture was different than the Georgians, and wanted independence. The Georgians denied their request, claiming that they had no right to a state in Georgia because they were a minority. As the conflict escalated to troop conflicts from both sides, the Soviet military got involved to work through a ceasefire. The Georgians claimed that the Soviets were helping the Ossetians to ensure that Georgia did not leave the Soviet Union. Regardless of the Soviet actions, Georgia declared independence in April on 1991. Hostilities between Georgia and South Ossetia continues until June 1992 when the post-Soviet Russians brokered a ceasefire between the two sides.

Despite the conclusion of that conflict tensions remained. Georgia looked west towards NATO for protection from their former occupiers, but South Ossetia remained in favor of cooperation with Russia. Similar ethnic divisions rose to the surface, and the Ossetians once again sought renewed independence from their perceived oppressors. Small skirmishes took place in the territory but the situation did not escalate to a full conflict until August of 2008 when Ossetian insurrectionists attacked the Georgian military. This act marked the beginning of brinksmanship between Georgia and South Ossetia that led to a large-scale military operation against the Ossetians.

The conflict between Georgia and South Ossetia was an issue for Russia. Russia saw Georgia's desire to join NATO as an aggression against them, and when several Russian peacekeepers were killed during the shelling of an Ossetian town, Russia used that as a justification for invasion. Prior to an invasion of troops, Russia used cyberattacks to weaken the Georgian military. "Security experts have identified two phases of the Russian cyber campaign against Georgia. The first phase commenced on the evening of 7 August when Russian hackers targeted Georgian news and government websites . . . the second phase, Georgian media and government websites continued to receive the attacks, but the Russian cyber operation sought to inflict damage upon an expanded target list including financial institutions, businesses, educational institutions, Western media (BBC and CNN), and a Georgian hacker website." (Shakarian, pg.63-64) The cyberattacks had a demoralizing effect on the Georgians. The cyberattacks against Georgia isolated them from the rest of the world in a time of need. By overwhelming Georgia's critical infrastructure, the Russians ensured that Georgia couldn't communicate the crimes to the west until it was too late. "Isolating Georgia from the outside world may also explain the attacks on Georgian banks that occurred during the second phase of cyber operations. At this time, several banks were flooded with fraudulent transactions. International banks, wanting to mitigate the damage, stopped banking operations in Georgia during the conflict.30 As a result, Georgia's banking system was down for ten days.31 This led to a shutdown of cell-phone services in the country—further isolating Georgia from the rest of the world.32 Russian hackers targeting Georgian business websites, also during the second phase, may have aimed to cause similar economic damage." (Shakarian, pg.66)

In addition to cyberattacks on critical systems, an information war blurred the lines between right and wrong in a way that hampered the west's ability to act. By taking advantage of public

opinion, the attackers gave Russia room to operate without drawing international condemnation. This type of isolation was an evolution of the strategies seen in Estonia, where critical infrastructure was attacked to prevent the government from operating efficiently.

The war ended with a ceasefire on August 12th, 2008. While the attacks were never directly attributed to the Russian government, the timing and effects of the attacks were distinctly related to Russian operations. The use of a cybercampaign as an auxiliary tool in coordination with traditional military force shows that this was a war. While the cyberattacks themselves were not enough to be considered warfare, their use to facilitate traditional warfare can be judged through Johnson's criteria for Just War. Looking at Johnson's criteria, was the Russian invasion of Georgia, and accompanied cyberwar justified?

Unlike the situation in Estonia, there is more substance to Russia's justification for aggression. Russia felt that Georgia was engaging in ethnic cleansing in the Ossetia region, and moved in to help them. In addition, when considering Russia's existential claims in Estonia, Russia felt their sphere of influence was under assault from the west. From the Russian perspective, there was just cause to go to war.

The intentions of a regional power are always suspect, but in the Russo-Georgian war there is little dispute. Russia saw an opportunity to bring peace to the region while ensuring the autonomy of a pro-Russian state on their border. They used military force to bring an end to decades of ethnic conflict. Russia had the right authority to engage the Georgian forces. By invading Georgia, Russia also managed to prevent Georgia from joining NATO. As both the largest power in the region, as well as an ally of one of the parties, Russia was justified in stepping in. "If Russia appeared as anything more than a peacekeeper for the breakaway regions,

the international community would be hesitant to support the independence claims that Moscow later made." (Ellison, pg. 350) Russia may have had wider goals in the region, but their actions kept to the motive of being international peacekeepers. However, Russia exceeded the proportionality of ends by targeting civilian populations with cyberattacks. Isolating a country from the international economy is an indiscriminate attack, and by neglecting to restrict their aggression to military targets Russia exceeded the proportionality of ends. The invasion of Georgia was not a last resort, but with a perceived ethnic cleansing of South Ossetians underway it is reasonable to infer that the situation was time sensitive. Had there been more information available sanctions could have been used to deter Georgia from engaging in hostile activities.

Russia had good reason to believe that their endeavors would be successful. With insurrectionists on the ground, and the Russian military extending into Georgia proper, there was a reasonable chance of success. Russia knew military action would end the ethnic conflict. From the Russian perspective, the Russo-Georgian war was fought to achieve peace for the South Ossetian people. While many in the international community condemned the invasion, Russia saw it as a means of putting an end to a decades long conflict.

Looking at Johnson's criteria for just war, Russia is only justified in their invasion of Georgia because of how narrowly IHL is interpreted regarding cyberaggression. If Russian cyberattacks during the campaign were considered acts of war, the indiscriminate targeting of civilians would show that Russian intervention expanded beyond the stated goals of protection, into a complete disruption campaign against Georgian society.

4. How to prevent this type of cyberaggression.

The post WWII period shows how IHL and MAD kept stability. With cyberweapons being developed countries who wish to assert geopolitical power now have the means to do so without fear of antagonizing outdated treaties. The disputed origins of cyberattacks serve as a screen for attackers to assault their victims with little repercussion. Considering the nature of NATO and IHL, the first step towards preventing these types of attacks should be deterrence. The world needs to write new laws that deter countries from engaging in cyberaggression, and when hosts in their country are found to be the source of these crimes, they need to be compelled to help the investigation. Russia claimed that they weren't responsible for the cyberattacks in Estonia, but when efforts were made to investigate by Estonian authorities, Russia declined to help. While they avoided international culpability, they obstructed the investigation in a way that strongly implies their involvement. Similarly in Georgia, while invading the country Russia denied that the cyberattacks were being led by them. This lack of accountability only serves to embolden state actors who wish to use cyberattacks to achieve geopolitical goals.

The integrated nature of digital infrastructure brings civilian and military targets closer together. International law needs to be updated to ensure that civilian populations are not unfairly targeted. The isolation of the Georgian people was inhumane, and by restricting their financial access the attackers almost created a refugee crisis. Citizens of Georgia couldn't escape the attacks without funds, and this restriction of civilian activity is functionally no different than the occupation of a territory.

In any war, information is key. This is especially true in cyberspace. "Relentlessly negative portrayals of the nation-state as an institution both disregard the positive attributes and accomplishments of the state system and ignore specific differences in how particular states are constituted and how they have behaved." (Johnson) An assault on accurate information puts

people in danger, and prevents peacekeepers from taking productive steps to save lives. As IHL sought to ensure that people who treated properly during war, a new addition needs to be discussed that enshrines the right to accurate information. “Information gathering and disruption have always been major tools of war. Disrupting an enemy's communications networks may even have greater strategic value than destroying its arsenals or supply lines. Indeed, some information warfare methods are considered so unsavory as to be prohibited by the laws of war.” (Swanson, 312) Without accurate information, there can be nothing but chaos and violence, and for a war to be just the aim needs to be peace.

Johnson’s criteria for Just War serves as a strong foundation for what should be just action in warfare. “As modern society increasingly relies on global and domestic information structures, these structures tend to become targets during war and other hostilities.” (Swanson, 305) Johnson’s criteria needs to be expanded to account for it. The cyberaggression against Georgia and Estonia show the path this type of warfare can take if left unchecked. From the purely digital intrusion of Estonian critical infrastructure, to a hybrid with Georgia that resulted in Georgia losing a part of its country, these attacks will only become more severe if the International community does not take a more direct approach to cybersecurity. It is imperative that the laws that govern war be reexamined through the lens of cyberwarfare, deterrence, criminal justice so that future conflicts can be averted.

Bibliography

Johnson, James Turner. "Just War, As It Was and Is | James Turner Johnson." *First Things*. N.p., 01 Jan. 2005. Web. 20 May 2017.

Brown, Gary D. "Proportionality and Just War." *Journal of Military Ethics* 2.3 (2003): 171-85. Web.

Klein, Bradley S. "Hegemony and strategic culture: American power projection and alliance defence politics." *Review of International Studies* 14.02 (1988): 133. Web.

Maras, Marie-Helen. *Cybercriminology*. New York ; Oxford: Oxford U Press, 2017. Print.

Ellison, and Brian J. "Russian Grand Strategy in the South Ossetia War." *Demokratizatsiya* 22 Sept. 2011: n. pag. Print.

Ruus, Kertu. "Cyber War I: Estonia Attacked from Russia." *European Affairs* 1 Jan. 2008: n. pag. Print.

Shakarian, Paulo. "The 2008 Russian Cyber Campaign against Georgia." *Military Review* 1 Nov. 2011: n. pag. Print.

Swanson, Lesley. "THE ERA OF CYBER WARFARE: APPLYING INTERNATIONAL HUMANITARIAN LAW TO THE 2008 RUSSIAN-GEORGIAN CYBER CONFLICT." *Loyola of Los Angeles International & Comparative Law Review* 32 (2010): 303-33. Web.

Thapar, Romila. "War in the Mahabharata." *Modern Language Association* 124.5 (2009): 1830-833. *JSTOR*. Web.

Toner, Christopher. "The Logical Structure of Just War Theory." *The Journal of Ethics* 14.2 (2010): 81-102. Web.

"UN Charter (full text)." *United Nations*. United Nations, n.d. Web. 20 May 2017.

Zehr, Nahed Artoul. "James Turner Johnson and the ‘Classic’ Just War Tradition." *Journal of Military Ethics* 8.3 (2009): 190-201. Web.