Russian Offensive Cyber Operations:

Dissecting International Relations Theory

Allison Moore

IR-6652 XTIA- Theory and Ideology in International Relations

May 21, 2022

Introduction

Since its first significant cyber operation in 1998 against the Wright-Patterson Airforce Base, Russia has devoted time and resources to establishing itself as a great cyber power (Alatalu, et al. 2018, 116). Throughout the 21st century, Russia has generated new tools, policies, procedures, and organizational structures to enhance its technical capabilities and to augment its kinetic capabilities through cyberspace. Recently, scholars have identified Russia's concept of hybrid war ('gibridnaya voyna') which stresses the importance of information operations and influence operations in cyberspace, in conjunction with conventional warfare (Fridman 2018, 94). This doctrine has been evidenced through Russia's application of aggressive cyber operations in Ukraine.

In 2015 and 2016, Russian cyber units conducted an attack of Ukrainian infrastructure which resulted in the loss of power for several hours (Buchanan 2020, 190-201). Russia has also applied cyber operations in support of its most recent invasion of Ukraine in 2022. Since January of 2022, Russia has conducted multiple "wiper" operations, seeking to delete important documents of the Ukrainian government; as well as attacks on Ukraine's infrastructure and electrical grid (Collier 2022). Considering these recent aggressive offensive cyber operations by Russia, I seek to review the conditions under which Russia decided to utilize its offensive cyber capabilities (OCOs), as well as predict the future of Russia's possible continued use of these OCOs and the international community's response from multiple theoretical views.

Below, I will assess the complex situation of Russia's use of aggressive OCOs from three theoretical perspectives. First, I will use the realist point of view to analyze the concept of Russian cyber power. Next, I will consider the constructivist approach, which is centralized around the concept of cybernorms. Finally, I will apply Marxism and the critical theories to uncover important additional actors to consider in the case of Russian abuse of cyberspace. Within each section, I will review the primary actors and conditions that led to Russia's decision to employ OCOs in Ukraine. I will also apply the fundamentals of each theory to predict how Russia's use of OCOs may change or remain the same in the future. Lastly, I will compare and contrast the strengths and weaknesses of each theory to determine which theory holds the most weight in the discussion.

A Powerful Cyber Reality

The first theoretical perspective I will consider is realism. The realist perspective applies significant authority to the role of power dynamics, specifically through state relative gains in power and security, within an anarchic international system (Atunes and Camisão 2017, 17). In the case of Russian OCOs, realism will tend to focus on the Russian state, with the goal of explaining why Russia might choose to conduct attacks in cyberspace. Realism offers little explanation of the international community's response to Russia's OCOs.

Russia seeks to gain and maintain the most relative power within its region, and- ideally- the entire international system. As the regional hegemon, Russia must ensure a balance of power as regional states seek to increase their capabilities. Due to the potential imbalance of power that may develop, Ukraine's efforts to join NATO is a direct threat to Russia's security and cannot go unchecked. To prevent Ukraine from gaining more power relative to Russia, the Russian state had to assert its power to deter Ukraine's attempts to upset the status quo in the region. The realist perspective contends that an aggressive maneuver by Russia would be responded to by aggressive maneuvers by other powers within the international system in an effort to balance power.

From the realist point of view, cyberspace is simply an extension of the physical domain and affords a unique area to demonstrate power and generate security. Cyberspace is quickly turning into an important arena to impact traditional kinetic operations; several states, to include Russia, have incorporated information and influence operations in cyberspace into their military and intelligence doctrine (Fridman 2018, 190-201). Simply stated, within the realist perspective cyber capabilities are equivalent to traditional military tools and equipment because they allow states an alternative method of asserting their power. State generation of increasingly sophisticated methods in cyberspace is comparable to a state increasing its military capacity. Because the tools and infrastructure required for cyber activities tends to be cheaper than traditional military equipment, cyber operations offer a unique opportunity for states to increase hard power while reducing the impacts on soft power.

Looking towards the future, a realist will likely assert that Russia will continue to leverage its cyber capabilities to ensure it remains a global cyber power. Furthermore, Russia will seek to develop more advanced cyber capabilities and will work to refine its cyber tactics, techniques, and procedures (TTPs). By retaining an advantage in cyberspace, Russia will ensure its ability to coerce other states to behave in a manner which is beneficial to the security of Russia. Realists will also highlight the expected continuance of Russia as the regional hegemon within Eastern Europe, as it will likely continue to assert dominance through cyberspace with the goal of becoming a great cyber power.

The Construct of Cybernorms

Next, I will explore the constructivist approach. Constructivism highlights the role of social norms and norm entrepreneurs in the explanation of actor behaviors (Theys 2017, 38). Considering Russia's aggressive use of OCOs, constructivists will home in on Russia as a norm entrepreneur. Furthermore, they will consider intergovernmental organizations (IGOs) and other prominent actors who may disagree with the precedent Russia is setting in cyberspace.

As technology becomes more advanced, e-Commerce and digital interactions become more and more common. The use of cyberspace has become a norm amongst governments, militaries, and intelligence communities across the system. Within the cyber domain, states and IGOs establish cybernorms which allow dominating entities

within the system to apply pressure on other states and organizations to adhere to those cybernorms. However, because there is no international cyber law, Russia has free reign to test the boundaries of these norms in cyberspace. As Russia explores these boundaries, it establishes itself as a norm entrepreneur, offering the international system a new standard.

The important question a constructivist will now ask is: will the rest of the international system allow Russia's cybernorms to enter into cascade (Finnemore and Sikkink 1998, 895)? If so, we will begin to see more states and organizations developing their offensive cyber arsenals. States will likely develop their own offensive cyber capabilities and consider implementing cyber-attack into their own warfare doctrine. We will also experience increased quantities of cyber-attacks and retribution in cyberspace as states and other cyber actors respond to OCOs with their own OCOs. In this version of the future, cyberspace has become the new 'wild west' and will only persist until a new cybernorm entrepreneur presents a better alternative.

However, should the system disagree with Russia's proposed norms, we can expect to see more progress towards the establishment of formal international cyber laws to ensure states remain within the current cybernorm framework. Constructivists also expect to see the creation of new IGOs to regulate cyberspace. Governance of cyberspace is a difficult topic and will require significant oversight, should the international community decide to seek international laws governing the use of cyberspace. These events are also expected in the previous scenario, once states, IGOs, and cyber actors become exhausted by the lack of regulation of cyberspace. Considering the constructivist point of view, Russia will likely continue to explore the

bounds of its cyber capabilities until the international community decides it doesn't agree with Russia's actions.

A Critic's Point of View

Finally, I will consider Marxism, critical theory and the perspective of mainstream theory critics. Unlike the theories discussed above, these theories take a look at individual perspectives. They consider marginalized people, place value on the experiences and opinions of those who lie outside of the traditional realm of international relations theory, and assert the idea of emancipating people from the modern system (Ferreira 2017, 49). Furthermore, they extend the scope of the issue to the entirety of cyberspace and the physical infrastructure required to support cyber operations. In the case of Russian cyber aggression, these theorists focus on the citizens who have suffered due to Russia's attacks against Ukraine.

Marxists highlight how the physical equipment required to access cyberspace requires significant reliance upon cheap labor in periphery and semi-periphery states. Computers and other hardware required to operate cyberspace rely heavily upon rare earth metals, of which China currently leads the world in mining and processing (Kirkpatrick 2019, 17-8). China is known for having somewhat relaxed environmental standards; some mining processes heavily pollute the surrounding area with "toxic sludge" (Ives 2013) and cause severe medical conditions for the citizens working in or living near these rare earth metal mines (Nayar 2021). Marxists likely consider these

individuals a modern proletariat suffering at the hands of bourgeoisie governments. Furthermore, the Marxist perspective draws attention to the possibility that these low wage workers may rise and overthrow the bourgeoisie, whose existence is not "compatible with society" (Marx and Engels 1888, I.).

Feminists draw attention to the lack of feminine input in the design and execution of cyberspace hardware and software (Smith 2017, 63). They also contend that the feminine perspective has been completely discarded and ignored in the decision processes on the use and implementation of OCOs, which fall into the category of "hard" issues (Smith 2017, 66). Furthermore, the feminist perspective highlights the individual Ukrainian citizens who were impacted by Russia's attack on the Ukrainian power grid. Power disruptions can cause significant issues and hardship, especially for low income and marginalized individuals. Some feminists may even highlight the impacts of Russia's OCO on Russian citizens who experience government censorship and misinformation. As Russian citizens speak out against Russia's actions in Ukraine- to include its use of cyber operations to influence Ukrainian and Russian citizens- they experience arrests, harassment, raids, detention, and prosecution from Russian law enforcement officials in an attempt to keep the Russian populace misinformed (Human Rights Watch 2022).

Looking towards the future, feminists will assert the importance of involving women and other minorities in the development of international cyber law, designed to combat the abuses of cyberspace evidenced by Russia's repeated attempts to impact Ukraine's physical infrastructure. They will also fight to incorporate more feminine perspectives in the development and implementation of technology-based systems by

fighting to include more women and minorities in the science, technology, engineering, and mathematics fields. Furthermore, feminists will draw attention to the human rights issues evidenced by the abuse of power within Russia and Ukraine; and they will work to reduce the impact of these abuses on the individual citizen. Marxists will fight to decrease the economic inequality throughout the system by contending for fair labor compensation for the workers in rare earth metal mines and other industries necessary for the development of cyber infrastructure. As briefly mentioned above, the Marxist perspective also alludes to the possibility of an uprising of LDC laborers who might fight for better living conditions and health care for those living around rare earth metal mines.

Not Created Equal: Where the Theories Fall

Through the discussions above, it is apparent that each theory holds important analysis for specific areas of the issue of Russia's use of OCOs. One theory is not inherently better than any other, unless we are looking to zoom in on a particular question regarding the issue. Below is a discussion on the strengths and weaknesses of each theory in comparison to one another. A full understanding of Russia's OCOs against Ukraine can likely be developed through the combination of aspects from each of the theories.

The realist perspective provides the best explanation for why Russia has chosen to attack Ukraine in cyberspace. Russia has always been a state focused on becoming

a great power which applies a tremendous amount of care for retaining substantial power relative to its neighbors (Renz 2018, 22-30). In this manner, the nature of Russia as a state and the behavior of Russia in international relations mirrors the realist theory. However, the realist theory focuses on the Russian state and biases analysis towards the Russian perspective. It does not provide suitable analysis of the international community's response to Russia's actions. Realism does not adequately consider factors outside of the Russian state, which greatly impacts the predictive power of the realist theory.

Constructivism shifts focus towards the non-Russian perspective and provides an excellent predictive power in determining how the international community might respond to Russia's actions in cyberspace. It also provides the best framework for understanding the role of cyberspace in international relations. As states develop new cyber capabilities and employ them, the international community responds by either adopting similar capabilities, or shunning the use of such capabilities. Although this theory provides predictive explanations for the masses, it does not provide fruitful consideration of the future path for Russia as the aggressor. Moreover, the constructivist perspective does a poor job of explaining Russia's reasons for initiating an OCO against Ukraine.

Marxism and the critical theories provide the best foundation for the individual perspective. They give voice to those who have suffered as a result of Russia's cyber aggression, both those working in rare earth metal mines and those who experience censorship by the Russian government. They elaborate on the role of economic inequality and the disproportionately low amount of minority influence over cyberspace

concepts, which are valuable perspectives in creating a more efficient and fairer cyberspace. However, these theories focus on the individuals on the receiving end of Russian action and do not provide an adequate depiction of the Russian state.

Constructivism, Marxism and the critical theories focus on those perspectives outside of the Russian state, while realism explains the Russian considerations at the state level. Together, all three of these theories provide for a more encompassing understanding of the situation and the possibilities for the future. Realism asserts the aggressive Russian state perspective, constructivism elaborates on the role of cybernorms, and Marxism and critical theories assert the importance of the feminine and marginalized points of view.

Conclusion

Over the last two decades, Russia has asserted its foreign policy through the use of aggressive offensive cyber-attacks. It has built up its cyber arsenal and committed time and money to establishing doctrinal rules and regulations governing its use of cyber capabilities in conjunction with kinetic force. Russia's recent use of OCOs against Ukraine provides an excellent opportunity to apply international relations theory.

Realism notes that cyber capabilities are comparable to traditional kinetic equipment and that these capabilities provide an alternative method for generating and exerting hard power. The realist perspective also highlights how cyber operations allow states to increase security through coercion of weaker states. Looking forward, realists

believe that Russia will continue to develop its cyber capabilities as they are an inexpensive method for developing hard power.

The constructivist approach draws attention to the role of the norm life cycle and portrays Russia as a norm entrepreneur in cyberspace. Constructivists assert that Russia will continue to develop new norms in cyberspace as long as the international community allows. However, the international community can prevent Russia's proposed norms from entering into cascade. Projecting into the future, constructivists note the possibility that the international community will call for international cyber law to prevent states from abusing their cyber capabilities.

Marxism and the critical theories take a step down to the individual level of analysis. They highlight the lack of involvement of feminine and marginalized perspectives in the development of cyber equipment, doctrine, and policy. Furthermore, they note the abuse of power in regard to the laborers who mine rare earth metals which support the manufacturing of cyber equipment, as well as the mistreatment of Russian citizens who work to correct Russian misinformation campaigns surrounding the Ukraine War. In the future, these perspectives call for more involvement of feminine perspectives, better working conditions for low wage workers, better environmental standards in rare earth metal mines and factories, and better treatment of individuals in Russia who speak out against the government.

This exercise of theory provides a better understanding of Russia's use of aggressive OCOs against Ukraine. Although there are some points of contention and areas left unexplained by the theories discussed above, current international theories can apply to cyberspace. Future analysis should be conducted on the remaining

international theories to determine which provides the best stand-alone perspective for understanding cyberspace and its use on the international stage.

Bibliography

Alatalu, Siim, Irina Borogan, Elena Chernenko, Sven Herpig, Oscar Jonsson, Xymena Kurowska, Jarno Limnell, Patryk Pawlak, Piret Pernik, Thomas Reinhold, Anatoly Reshetnikov, Andrei Soldatov, and Jean-Baptiste Jeangene Vilmer. 2018. "Conclusion Russia- From Digital Outlier to Great Cyberpower." eds. Nicu Popescu and Stanislav Secrieru, *Hacks, Leaks and Disruptions: Russian Cyber Strategies.* European Union Institute for Security Studies (EUISS). http://www.jstor.org/stable/resrep21140.15. (Accessed April 7, 2022).

Antunes, Sandrina and Isabel Camisão. 2017. "Realism." In *International Relations Theory.* Eds Stephen McGlinchey, Rosie Walters, and Christian Scheinpflug. Bristol: E-International Relations Publishing.

Buchanan, Ben. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Cambridge: Oxford University Press, 2020.

Collier, Kevin. 2022. "Ukraine Says Russian Cyberattack Sought to Shut Down Energy Grid." *CNBC.* https://www.cnbc.com/2022/04/12/ukraine-says-russian-cyberattack-sought-to-shut-down-energy-grid.html. (Accessed April 23, 2022).

Ferreira, Marcos Farias. 2017. "Critical Theory." In *International Relations Theory.* Eds Stephen McGlinchey, Rosie Walters, and Christian Scheinpflug. Bristol: E-International Relations Publishing.

Finnemore, Martha and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization.* 52(4): 887-917. doi:10.1162/002081898550789.

Fridman, Ofer. 2018. *Russian 'Hybrid Warfare'***:** *Resurgence and Politicisation.* New York**:** Oxford University Press.

Human Rights Watch. 2022. "Russia: Arrests, Harassment of Ukraine War Dissidents." https://www.hrw.org/news/2022/03/24/russia-arrests-harassment-ukraine-war-dissidents. (Accessed May 21, 2022).

Ives, Mike. 2013. "Boom in Mining Rare Earths Poses Mounting Toxic Risks." *Yale Environment 360.* https://e360.yale.edu/features/boom_in_mining_rare_earths_poses_mounting_toxic_risks. (Accessed May 18, 2022).

Kirkpatrick, Keith. 2019. "Electronics Need Rare Earths." *Communications of the ACM.* 62(3): 7-18. DOI: 10.1145/3303847.

Langner, Ralph. 2016. "Cyber Power: An Emerging Factor in National and International Security." *Horizons: Journal of International Relations and Sustainable Development*. 8: 206–218. https://www.jstor.org/stable/48573698.

Marx, Karl and Friedrich Engels. 1888. “The Communist Manifesto.” *The Project Gutenberg eBook of the Communist Manifesto by Karl Marx and Friedrich Engels*. https://www.gutenberg.org/cache/epub/61/pg61-images.html. (Accessed April 23, 2022).

Nayar, Jaya. 2021. “Not So ‘Green’ Technology: The Complicated Legacy of Rare Earth Mining.” *Harvard International Review.* https://hir.harvard.edu/not-so-green-technology-the-complicated-legacy-of-rare-earth-mining/. (Accessed May 14, 2022).

Pernik, Piret, Siim Alatalu, Irina Borogan, Elena Chernenko, Sven Herpig, Oscar Jonsson, Xymena Kurowska, et al. 2018. “The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine.” In N. Popescu & S. Secrieru (Eds.), *HACKS, LEAKS AND DISRUPTIONS: RUSSIAN CYBER STRATEGIES* (pp. 53–64). European Union Institute for Security Studies (EUISS). http://www.jstor.org/stable/resrep21140.9.

Renz, Bettina. 2018. *Russia’s Military Revival.* Cambridge, UK: Polity Press.

Smith, Sarah. 2017. “Feminism.” In *International Relations Theory.* Eds Stephen McGlinchey, Rosie Walters, and Christian Scheinpflug. Bristol: E-International Relations Publishing.

Theys, Sarina. 2017. “Constructivism.” In *International Relations Theory.* Eds Stephen McGlinchey, Rosie Walters, and Christian Scheinpflug. Bristol: E-International Relations Publishing.