UNJPE

University of Nigeria Journal of Political Economy: Volume 11, 18-21 (2021)

Cyber Attack as a Tool to Influence Foreign Policy: A Comparative Study of Russia's Cyber-Attacks on Estonia and Georgia

Ejimofor Maurice Odoh
School of Governance, Law, and Society, Tallinn University, Estonia
odohejimofor@gmail.com; momotlu@tlu.ee

Abstract

In recent years, cyber warfare deployment has formed part of the integral discourse in international affairs between states and foreign policy interactions. This study examines Russia's deployment of cyberattack as a warfare strategy aimed at influencing other states' behavior as well as asserting its dominance in its geopolitical space against the Western alliance. Cyberwarfare strategy in the context of this study is aligned with the proponents of 'sharp power' mechanisms in state interactions. The study conducted a comparative study of Russia's cyberattacks on Estonia in 2007 and Georgia in 2008. The objective of the study is to look at the implications of Russia's cyberattacks on both Estonia and Georgia and how successful these attacks have been in shaping the foreign policy objective of Russia, and by extension, influenced the domestic behavior of Estonia and Georgia.

Keywords: Cyberwarfare, cyberattack, foreign policy, cyber defence, geopolitics

Introduction

The issues of cyber-attack and cyber warfare have come to dominate international political discourse in recent times and this is due to its use as a means to influence the behavior of a state by another. The cyber capability of any state is dependent mostly on its ability to deploy it in defense strategy. Thus cyber defense is the main aim of why states invest in sophisticated cyberinfrastructure to enhance their cyber domain. It is essential to assert that cyber defensive mechanisms can also translate to a cyber offensive strategy whichever way suits the objective of the state at the time.

The use of cyber power strategy by states, especially states with access to sophisticated cyberinfrastructure and dominance like Russia, United States, and so forth, is geared towards utilizing it as an instrument to shape their foreign policy goals and towards influencing the behavior of their targeted state or institution in their international relations. This act is carried out as an attempt to avoid the use of conventional military deployment to engage the targeted state in a diplomatic fallout. The risks and escalations

involved are hardly measurable because of the challenging issue of attribution and established international regimes that can address the use of cyber offensive strategies in diplomatic fallout or conflict situations. The foreign policy objective of every state is practically the objectives of the state as it relates to others and the means of achieving them. Drawing from this, a cyber offensive strategy can be seen in this case as part of a means in advancing the foreign policy goals of a given state. Russia is a typical case of how states deploy cyber offensive strategies to drive their foreign policy ideas, especially in its geopolitical sphere.

Russia's cyber capabilities can best be understood through its approach to cyber warfare and all the attendant strategies that is been used to project its foreign policy objectives, especially towards the west, NATO, and the European Union (EU). In recent years, Russia has been able to demonstrate its ability to redefine and incorporate cyber warfare as part of its military warfare strategy, this is why it could launch offensive cyberattacks on Estonia in 2007 and Georgia in 2008. The kind of cyberattack tactics used on both Estonia (cyberattack of critical infrastructure, DDoS) and Georgia (information warfare, DDoS) are similar but the overall strategy is different and can be said to be a part of Russia's hybrid warfare strategy. One would wonder why Estonia was a target of Russia's cyberattack and why was Georgia a target too? Russia has been developing digital technology to keep an eye on the political events that are happening within Russia and to also monitor international political events especially in its geopolitical region with a clear strategy on how to avoid the kind of regime change that took place across the Arab states of North Africa and the Middle East (Egypt, Tunisia, Libya, and Yemen) with the help of digital media and technologies (Nocetti, 2015). Furthermore, Russia saw the use of the internet as a fundamental tool in the hands of the United States and especially with their relationship with the US allies and its neighbors, and if not checked it can be a medium to

infiltrate Russia's political space thereby rendering it vulnerable. These among others informed the decision for Russia's development of digital infrastructure in furtherance of its political goals in its geopolitical space and to maintain a strong grip on its domestic politics.

Cyberwarfare was deployed by Russia on its neighbors, Estonia and Georgia, to destabilize these states while exposing their vulnerability and to maintain an underlying dominance in geopolitical affairs. The central question is, can cyberattack be used to shape foreign policy to successfully coerce other states' behavior? The paper will be looking at the implications of Russia's cyberattacks on Estonia and Georgia and how successfully Russia has been able to deploy cyber warfare strategy to boost its foreign policy objectives. The paper will be structured by first looking at Russia's cyber warfare strategy as a tool of foreign policy; Russia's cyberattack on Estonia: Reactions and implications; Russia's cyberattack on Georgia: a combination of cyberwarfare and military campaign, factors and impact; and conclusion.

Russia's Cyber-Warfare Strategy as a Hybrid Warfare Tool to Shape Foreign Policy.

Since the end of the Cold War, Russia has struggled to maintain its influence on its sovereign powers and to match the aggressive intrusion of the west in its geopolitical space. There has been increased western presence in the Eastern European region both in the military (NATO) and other diplomatic approaches, especially with states who share boundaries with Russia, and this move is perceived by Russia as a way of the West, in this case, the United States, EU, and NATO, influencing its neighbors' domestic political and foreign policy which may invariably render Russia vulnerable to the west. This has propelled Russia to reorganize its domestic political doctrine by utilizing the information

tool and developing cyber defense infrastructure to respond to and against an existential threat from not just within its territory but also from the external (Connell & Volger, 2017, p. 3).

In a bid to establish itself as a world power with particular interest across Europe and Eurasia, Russia developed its kind of hybrid warfare to counter the diplomatic, digital, and information threat posed by the west. Hybrid warfare in this case refers to Russia's application of non-conventional military warfare, such as information, economy, propaganda, population, and cyber warfare, to promote the national interest of Russia. Hybrid warfare can also be referred to as 'sharp power'- which can be simply defined as the tools and strategies that are used for achieving foreign policy objectives through the use of hybrid war strategies of propaganda, psychological and other methods without and deployment of military weapons (Meister, 2016, p. 7). Sharp power mechanisms involve the attempt of one state to manipulation another through the various medium which includes media manipulation, misinformation, and use of digital elements in advancing their interest and control (Walker, 2018). Thus the need for the development of Russia's cyber defensive mechanism in furtherance of its set out foreign policy objectives which is to protect its influence in its geopolitical space, weaken the NATO alliance, and sow seeds of discord within the European Union and this is achieved by targeting individual member states of these organizations, like Estonia, Georgia, and Ukraine among others. Russia's hybrid warfare or what General Gerasimov called the 'new generation warfare', has been deployed as offensive strategies on unsuspecting states in the international system through instruments of power most especially information and cyberattack strategies hacking DDoS, and other tools of maintaining regional power and hegemony (Chivvis, 2017, p. 1).

With the use of sharp power mechanisms, Russia could afford to match and counter hybrid threats from its perceived enemies. Russia recognizes the fact that it may not be able to stand any chance in conventional military capability with the transatlantic forces thus resorting to deploying soft power tactics to achieving its aim. Sharp power tactics like the use of cyber warfare or cyberattack strategy are one of the most evident base methods that Russia has used as an offensive tool in pursuing its interest and influencing its target states or entity across the world (Ajir & Vailliant, 2018, p. 74). Cyber power is a viable tool for Russia towards a successful implementation of its covert foreign policy strategy in destabilizing the internal political system of its target state by initiating the various cyberattack tactics ranging from information warfare which is the use of social media, conventional media, DDoS (Distributed Denial of Service), an attack on digitalized critical infrastructures.

The rationale behind Russia's use of cyber warfare to pursue its foreign security policy and interests (and by also influencing the behavior of the targeted state) is to avoid as much as possible the use of physical force or physical military warfare in the event of a fallout from a diplomatic row. Certain groups have been identified as being sponsored by the Russian government in carrying out these cyber offensive strategy and they include, hackers (who have nationalist or political ideas, known mostly as hacktivists) (Connell & Volger, 2017, pp. 3-7), trolls and anonymous internet and social media influencers among others. The preference for hackers and other groups to execute these attacks is because it is less expensive to use proxies and it may only require just providing them technical support while keeping the state in an anonymous position. Also, it provides Russia the opportunity to operate within the grey zone of information warfare in cyberspace (Ibid, p. 11).

The objective of Russia's cyberattacks and offensive on all its target remains the same but its tactical methods vary from case to case depending on the target and intended outcomes. Subsequent sections will look at how Russia introduced cyber offensive strategies on Estonia and Georgia and the various methods that were used. The comparative study will show if the level of success Russia could muster through this cyberattack strategy on Estonia and Georgia.

Russia's Cyber Attack on Estonia: Reactions and Implications

In April 2007, Estonia's critical infrastructures, state institutions, and media outlets among others were attacked in what we regard as a cyberattack. The attack was carried out just a day after the Estonia government resolved to relocate a Soviet World War II memorial statue, which is located within the central part of Tallinn, Estonia's capital, to a military cemetery. This resulted in a clash between some Russian-speaking youth protesters and the Estonian government. The Russian government expressed their displeasure to the Estonia government on their decision and this created a crack in the diplomatic relations of both states. The escalations got to the level where the Estonian Ambassador to Russia was physically attacked in Moscow and the Estonian Embassy in Moscow was also attacked by hostile and angry Russian youths (Pernik, 2018, p. 55). Subsequently, misinformation and distorted news about the government of Estonia and its officials began to find their way into people's phones and other media platforms especially in Russian-speaking social media and internet platforms. All these were done to discredit the Estonian government and to coerce them to rescind their decision on the movement of the WWII monument from the center of Tallinn to anywhere, but the Estonian government had resolved to push forward with their plan. In the midst of all these, a devastating cyber-attack was launched against Estonia, where the official

websites of the government, political parties, government officials as well as critical service sectors like the banks and financial institutions were also affected. The cyberattack was said to have been carried out by random hackers who are sympathetic to the patriotic ideals of Russia and also were backed by the Russian government.

The disruptions were caused by Distributed Denial of Service, DDoS, unleashed on the Estonian government and service sectors. The result of the cyberattack left the Estonian state vulnerable and the government and critical service infrastructure were shut down for seral days. Amid the cyberattack on Estonia, the Russian President, Vladimir Putin, issued a very threatening statement where he accused the Estonian government of displaying the Hitler kind of Nazi regime with total disregard to its peoples (Bright, 2007). The cyberattack aims to halt government and businesses in Estonia and to fuel malicious propaganda against the Estonian government and its officials to reveal their vulnerability and thereby influencing their behavior. Although Estonia is said to be a digitalized society and is said to be the best in Europe in the e-governance system, it fell short of its cyber defense strategy which could have prevented these large-scale cyberattacks on its cyberspace. Even though some of the attacker's IP addresses were traced to Russia, the Estonian government could not hold on to any feasible evidence of direct Russian government involvement in the cyberattack. This is one of the challenging factors in cyberattack and warfare, retribution.

Estonia was able to recover from these attacks but not without fears of future attempts unless there is a collective effort by the international community to establish international regimes that will regulate cyberattacks and deter cyber oppressors, just like it is with the nuclear and conventional wars. Estonia was able to coordinate all resources together to respond to the cyberattack by establishing a Computer Emergency Response

Team that was at the forefront (Ashmore, 2009, pp. 6-7). They were able to mitigate the attack but what does it hold for both Estonia and its allies? How and what are the kind of cyber defensive mechanisms that should be put in place to deter such a wide-scale attack in the future? The impact of the cyberattack was mostly felt by the government and financial sector, the people and government officials were also affected and it took a long while to get over the shock. NATO as an ally also felt the impact and has been advocating for the need to critically deter cyberattacks especially on its members, but the question is how do you deter cyberattacks?

Russia's Cyberattack on Georgia: A Combination of Cyber Warfare and Military Campaign: Factors and Impact

The impact of the 2008 cyberattack on Georgia took a heavy toll on the government, media, infrastructure, and the people when compared to the Estonia experience. Both Estonia and Georgia experienced DDoS cyberattacks but the factor that distinguished both states' experiences is the combination of both cyberattack and conventional military warfare employed by Russian in Georgia. The cyberattack was on a large scale in Georgia ranging from the website of the president to trolling on social media platforms and so forth. In July 2008, hackers gained access to the website of the President of Georgia, Mikheil Saakashvili, and defaced his image and other insignias with the pictures of Adolf Hitler and eventually took control of the website for up to 24 hours (Ashmore, 2009, p. 10). Subsequently, an orchestrated Distributed Denial of Service, DDoS attack was launched against official government websites, especially the National Bank of Georgia and that of the Foreign Affairs Ministry, where their websites were defaced with images of Nazi signs and Adolf Hitler all over the sites. Georgia could not defend itself adequately because of the absence of advanced cyberinfrastructure that could confront such attacks.

The leading event that led to Russia launching such an attack on Georgia was to provide support to the Russo-Georgians who are mainly Russian-speaking Georgians and have been fighting for their autonomy from Georgia since they declared independence in 1991. Russia has always been sympathetic to its course simply because of its identity and affiliation (King, 2008). Series of conflicts have erupted over the years especially in 2004 and 2008, but in 2008, Russia used cyber and information warfare strategy combined with military intervention to lend support for South Ossetia forces

In August of 2008, large-scale attacks on the news media, internet, social media platforms, and government websites. The second cyberattack was carried out whilst the same period the Russian military troops invaded Georgia in South Ossetia. The strategy employed by Russia was to destabilize the Georgian government and create an environment where they will be exposed and vulnerable and while this was going on, they will be distracted and thus enabling the invasion of their (Russia's) military troops into South Ossetia (Kozlowski, 2013, p. 238). Russia's cyberattack used botnets (the domain used by the hackers to launch the attack on Georgia) with professional help from hackers to weaken the government of Georgia in their attempt to respond to the attack. Certain factors were at play which led to the successful cyberattack by Russia (Ibid, p. 239)- first, the Georgian state's digital infrastructure was not sophisticated enough to respond to the attack; secondly, Russia planned to weaken the political system within Georgia by defaming, trolling and manipulating information to create distrust amongst the people against their government and officials; also, the cyber-attack could be said to be a tactic to distract and overwhelm Georgia to weaken their defense during the military campaign and invasion.

Russia utilized information warfare on Georgia very successfully because its target was to create a breach in communication between the government and the people, take control of the media and all other internet communication platforms where they fueled more falsehood about the Georgian government officials and institutions, also to showcase how vulnerable and weak the Georgian state is including its leaders. Information warfare is a very significant tactic in cyber warfare and the level of how Russia deployed it on Georgia shows how effectively dangerous it could influence the conduct of the target state and as a tool for an aggressor. During these attacks, the economy of Georgia suffered immensely, however, realizing the hopeless situation they have been subjected to, Georgia decided to reach out to other states for help. States like Estonia tried to help by fixing their websites and restore their digital systems, also the United States assured the Georgian President of financial aid to help revive their economy.

Conclusion

The cyberattack has now come to be globally seen as a great threat to a state's sovereign existence and it's a vital tool that can expose the vulnerable position of a target state by an aggressor. Russia used cyber warfare tactics as a tool in protecting its domestic political dominance and to ward off any perceived threat that may likely threaten its geopolitical influence, and this posture is seen in Russia's cyberattack on Estonia and Georgia. Although the tactics employed by Russia may vary both in Estonia and Georgia, the main objective and strategy remained the same. The success of the cyberattack could be traced to some factors ranging from the presence of a large Russian speaking population present in both Estonia and Georgia which aided and amplified the attack because of their sentimental attachment to Russia and the good use of information warfare tactics played a huge part in charging these people against the government of

both target countries. For instance, the reactions that greeted the removal of the Bronze Soldier in Tallinn, Estonia, and the use of social media trolls and platforms to smear the Georgian government.

Another factor is the vulnerable state of the digital infrastructures of both Estonia and Georgia at the time of the attack. Both countries experienced DDoS attacks from the Russian-sponsored hackers and this is because Russia has more sophisticated defensive and offensive cyber capabilities which they applied very boldly on both countries. The strategy was to influence the domestic political situations in both states in other to promote their presence and interest in the possible outcomes of such an attack. Furthermore, the hacking of the websites of the government institutions and officials of both counties was due to the weak internet and cyber defense mechanism in place, thus exposing the weak posture of these states to Russia's attack.

In all, these attacks have similar factors and the tactics employed by Russia are also similar to some extent except were in Georgia, Russia used both cyber warfare and military troops to supplement the attack on Georgia to assist the South Ossetia forces. In summary, Russia was able (to some extent) to use cyberattack as a tool to influence events within the political and socio-economic situations in both Estonia and Georgia, the strategy was effectively deployed but does it prove to be successful in influencing the behavior of Estonia and Georgia? Well, the aftermath of the attack shows that both states have understood the dangers in cyberattacks whilst Estonia has stepped up its cyber defense mechanisms while Georgia seems to have lost Southern Ossetia.

References

Ajir, M., & Vailliant, B. (2018). Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly, 12*(3), 70-89.

Ashmore, W. C. (2009). Impact of Alleged Russian Cyber Attack. *Baltic Security and Defence Review, 11*(1), 4-40.

Bright, A. (2007, May 17). *Estonia Accuses Russia of 'Cyberattack'*. Retrieved March 30, 2020, from The Christian Science Monitor: file:///C:/Users/admin/Downloads/Estonia-accuses-Russia-of-cyberattack-CSMonitor.pdf

Chivvis, C. S. (2017). *Understanding Russia "Hybrid Warfare": And What Can Be Done About It.* Santa Monica, CA: Rand Corporation.

Connell, M., & Volger, S. (2017, March 01). *Russia's Approach to Cyber Warfare.* Retrieved March 29, 2020, from Defence Technical Information Center: https://apps.dtic.mil/docs/citations/AD1032208

King, C. (2008). The Five-Day War: Managing Moscow After the Georgia Crisis. *Foreign Affairs, 87*(6).

Kozlowski, A. (2013). Comparative Analysis of Cyberattacks on Estonia, Georgia, and Kyrgystan. *International Scientific Forum, ISF 2013. 3*, pp. 236-245. Tirana, Albania: European Scientific Institute, ESI Publishing.

Meister, S. (2016). *Putin's Version of Soft Power: Isolation and Propaganda.* German Marshall Fund of the United States.

Nocetti, J. (2015). Russia's 'Dictatorship-of-the-law' Approach to Internet Policy. *Internet Policy Review, 4*(4). DOI:DOI: 10.14763/2015.4.380

Pernik, P. (2018). The Early Days of Cyberattacks: The Cases of Estonia, Georgia, and Ukraine. In N. Popescu, & S. Secrieru, *Hacks, Leaks and Disruptions: Russian Cyber Strategies.* Paris: EU Institute of Strategic Studies.

Walker, C. (2018). What is Sharp Power? *Journal of Democracy, 29*(3), 9-23.