Journal of Innovations in Educations and Social Sciences
Leruse Newsy Associates
Volume 3. Issue 1 https://jiess.org ISSN:3006-6603

Hybrid Warfare and Information Operations as Core Tools of Russian Foreign Policy

Farwa Riaz[1]
Bachelor scholar, Department of political Science & International Relations, Government College Women University, Faisalabad, Pakistan
Email: chulbul2452@gmail.com
Dr. Sidra Karamat[2]
Lecturer, Department of political Science & International Relations, Government College Women University, Faisalabad, Pakistan
Email: sidrakaramat@gcwuf.edu.pk
Syed Tanveer Ali Shah[3]
Lecturer, Department of Politics and International Relations, University of Sialkot, Sialkot, Pakistan
Email: syed.tanveerali@uskt.edu.pk

ABSTRACT

In the contemporary security environment, hybrid warfare has become a significant instrument of statecraft, combining conventional military capabilities with cyber operations, information campaigns, economic pressure, diplomatic influence, and other non-military tools to achieve strategic objectives. This study examines how Russia has integrated hybrid warfare and information operations into its foreign policy to advance national interests and influence regional and international affairs. The research explores the evolution of Russia's hybrid warfare strategy, emphasising the use of disinformation, cyber operations, strategic communication, media influence, and political narratives to shape public opinion and weaken the cohesion of rival states. Based on a qualitative and analytical methodology, the research is based on academic articles, official reports, and reliable secondary sources. Russia has a history of using these strategies in practice as demonstrated in case studies of Crimea, Eastern Ukraine, Syria, and Western election interference. The theoretical frameworks such as the Theory of Realism, Hybrid Warfare Theory, Information Warfare and Strategy Communication are all used to support the analysis of the approach used by Russia in the contemporary conflict. Results indicate that the hybrid strategies of Russia are systematic, flexible and highly coordinated, such that they allow it to manipulate states and promote foreign policy interests without necessarily engaging in large-scale conflict. The knowledge of these techniques is important to the policymakers, experts and researchers trying to develop resilience and enhance global stability.

Keywords: Hybrid Warfare, Information Operations, Russian Foreign Policy, Cyber Warfare, Disinformation, Strategic Communication

Introduction

The twenty-first century has turned into the era of Hybrid Warfare and Information Operations as the insignia of the foreign policy of Russia. With the evolving nature of global politics, whereby the wars are no longer based on battlefield, the states have now been compelled to extensively use covert, indirect, and non-military means to gain influence and undermine their rivals. Russia, especially, has become one of the most developed and regular followers of this contemporary policy (Johnson, 2018). Hybrid warfare is the combination of various tools such as military coercion, cyber activities, propaganda, energy, diplomacy, financial instruments, and covert actions that are used to accomplish the political goals without the development of the full-scale war. Information operations also augment this strategy by informing the masses, controlling the narratives, and introducing confusion strategies in the specific societies. Combined, these two factors enable Russia to fight with its competitors, oppose the influence of the West, and defend its geopolitical interests without incurring the high prices and risks of the traditional war (Mumford, 2017).

The transition to hybrid approaches in Russia is based on the past and the changing security landscape. With the fall of the Soviet Union, Moscow was confronting the movement of NATO, economic depression and less global prominence. It also did not depend only on the conventional military might, which Russia could not possibly keep up with when compared to the Western nations, but instead aimed to come up with more sophisticated and more adaptable plans (Galeotti, 2018). General Valery Gerasimov and other Russian military intellectuals stressed on the role of information supremacy, psychological control and the political war in the present-day conflict. Such thinking led to one more model: battles are fought not only by weapons but also by the media, cyberspace, diplomacy, and influence on society. The information was turned into a potent tool to manipulate the decision-making process, interfere with internal division, and undermine the confidence of an opponent internally (Hoffman, 2009).

One of the main aspects of the hybrid strategy in Russia is the informational operations. These are disinformation, fake news channels, online propaganda, hacking into, influencing via social media, and controlling the narrative using state-controlled media such as RT and Sputnik (Bettina, 2016). The point of doing this is not just to convince, but also to confuse, to make people hard to agree what is the truth and what is the lie. Russia is using the existing social differences, promoting the political tension, and the lack of trust in the democratic institutions. In the run up to elections in countries all over the globe, Russian sponsored campaigns have tried to manipulate votes to gain, hurt reputations, and push agendas that would benefit Moscow. Through manipulation of information landscape, Russia aims at establishing a strategic edge but does not utilize massive armies (Thornton, 2015).

A combination of covert military actions and irregular forces is also a part of hybrid warfare. In Ukraine since 2014, Russia deployed unmarked soldiers (so-called little green men), militias of local forces, and cyberwarfare and massive disinformation to legitimize the annexation of territories and the contribution to separatist activities (Mansoor, 2012). Russia in Syria used military assistance to the Assad administration together with the information campaign, which

projected it as a stabilizing force against terrorism. It employs private military groups like Wagner group in Africa and the Middle East to extend its influence without being detected. This model gives Russia the opportunity to play aggressive but not to take direct responsibility and face international law (Margaret, 2007).

There is also a role of Economic and political tools. Russia is one of the largest natural gas exporters globally and she employs the natural gas supplies, oil contracts and the energy pricing as the pressures and rewards instruments (Russell, 2009). Russia is likely to have a more significant influence on the nations that rely on its energy. The course of diplomatic messaging and intelligence activities also ensures the power of Russia and enables it to use the vulnerabilities of the opponent and manipulate the discussions in its favor (Jonsson, 2019).

The cost-efficiency of hybrid warfare is one of the primary factors that underpin the centrality of this warfare to the Russian policy. Propaganda campaigns and cyber operations also do not need many resources in comparison to conventional war but can have serious political, economic, and psychological effects (Russell, 2009). These are the instruments that enable Russia to exert power outside of its immediate location, extending to Europe to Africa and the United States even amidst the economic sanctions and demographic troubles in the home country. Notably, hybrid operations are typically not yet beyond the limit of open conflict, minimizing the potential risk of retaliation being on a large scale (Bousquet, 2017).

Hybrid Warfare and Information Operations have turned into a principle tool of Russian foreign policy as they enable Moscow to reach strategic objectives in only subtle and flexible ways including those that remain unseen. Putting together cyber capabilities, media manipulation, political pressure, and a low involvement in military affairs, Russia is able to influence global events, destabilize other players and advance its own geopolitical narrative at a considerably lower cost than direct confrontation (Johnson, 2018). During the time when the boundaries between war and peace are more than ever obfuscated, the hybrid approach of Russia is a crucial aspect of modern international relations that should be used to analyze the contemporary international relations and to understand what should be expected in the future (Mumford, 2017).

Historical Background

The history of how Hybrid Warfare and Information Operations were utilized by Russia is based on the geopolitical, military, and ideological changes that occurred after the fall of the Soviet Union in 1991. The collapse of the USSR not only terminated the Cold War but also significantly diminished the world power and economic potential as well as military might of Russia. The political instability, the economic downturn, weaker state institutions, and the loss of control over the former Soviet republics were the problems that Russia faced during the 1990s (Mansoor, 2012). Meanwhile, the policy of NATO expansion to the East and the Baltic countries was viewed by Moscow as strategic threat. This created a profound feeling of weakness and longed to get back Russia to its position as a leading world power, without the economic or military strength to engage in direct conflict. It was in this atmosphere that Russia began to be

oriented toward low cost, indirect, and flexible forms of influence - subsequently called hybrid warfare (Mumford, 2017).

In the early 2000s, during the tenure of president Vladimir Putin, Russia's military was being reconstructed, its state institutions were reorganized and its central power over media and intelligence consolidated. Russia had discovered that contemporary wars were more reliant on information superiority, technological abilities and political control than on conventional power of the battlefield (Galeotti, 2018). This reasoning was boosted further by witnessing the Western military operations in Iraq, Afghanistan and Kosovo where the United States and NATO applied precision technology, psychological operations and media tactics successfully. The Russian military planners came to the conclusion that the modern war would be won using both military and non-military weaponry, primarily the weaponry capable of controlling the perception and destabilizing the societies and narratives (Hoffman, 2009).

This changed in the mid-2000s when a wave of color revolutions struck the countries of Georgia 2003, Ukraine 2004, and Kyrgyzstan 2005. These pro-democracy uprisings were seen as western backed to undermine Russian influence in its classic spheres by Russia. To this, Moscow increased its progression of hybrid strategies that were intended to thwart any similar movement not only at home but also in the outer world. The following strategies were involved: manipulation of local media, building cyber capacity, and the introduction of infrastructure of state-sponsored propaganda and disinformation (Bettina, 2016).

In 2014, when Crimea was annexed, and the conflict in Eastern Ukraine started, the hybrid doctrine of Russia was finally seen at the international level. A mix of unmarked soldiers, local militia, political pressure, economic pressure, cyberattacks, and huge disinformation campaigns was used by Russia to legitimize their actions and destabilize Ukraine (Thornton, 2015). This was the initial significant exposition of the modern hybrid warfare model of Russia. These same techniques would be used in the future in the Syrian conflict, European politics, the Middle East, Africa, and even in so-called attempts to influence Western elections (Mansoor, 2012).

Overall, Russian hybrid warfare strategy history is dictated by the post-Soviet insecurity, geopolitical competition with the West, experience of the past wars, and even a conscious choice of renewing its approach to the impact on the world processes. Gradually, Russia has built a complex regime that combines information work, cyber weapons, political influence, and undeclared military intervention; thus hybrid warfare became the focus of their foreign policy (Margaret, 2007).

Theoretical Framework

The theoretical approach to the study of Hybrid Warfare and Information Operations as Core Tools of Russian Foreign Policy consists of the combination of various points of view related to international relations, military strategy, and communication studies (Jonsson, 2019). The concept of realism reasons why Russia is concerned with power, survival, and national interest and why hybrid approaches provide the ability to influence without the outright warfare. The

Hybrid Warfare Theory (Gerasimov Doctrine) focuses on the ability to integrate military, cyber, political, economic, and covert capabilities to meet the strategic objectives in the gray zone between war and peace. The Information Warfare Theory demonstrates the effectiveness of propaganda, disinformation, and manipulating the media to influence the opinion of the masses and undermine the opponents (Russell, 2009). Strategic Communication Theory describes how Russia has been strategically communicating to legitimize actions and persuade the external audience. The theories of soft and Sharp Power explain how Russia has a combination of attraction, influence and cerements to destabilize other nations. Cyber Warfare Theory gives emphasis on digital attacks as affordable, deniable resources to aid hybrid strategies. These theories combined offer a platform through which we can define the multidimensional approach of Russia with information and indirect methods as the core elements in attaining the foreign policy goals (Bousquet, 2017).

Discussion

The paper demonstrates that the application of hybrid warfare and information operations by the Russian is a calculated and tactical aspect of its foreign policy, in order to accomplish the goals of geopolitics without direct military conflict. The use of hybrid warfare enables Russia to use a synergized strategy through the use of military, cyber, economic, political, and informational capabilities to bring about ambiguity which restrains the ability of adversaries to retaliate. The effectiveness of such strategies is augmented by information operations such as the use of propaganda, disinformation, and manipulation of the media, which affect the way people perceive things, turn societies polar and undermine institutional trust (Russell, 2009). Examples of Crimea, Eastern Ukraine, Syria, and Western election interference indicate that such operations are extremely flexible and context-dependent and take advantage of the weaknesses of target states. The examples of such theoretical approaches as Realism, Hybrid Warfare Theory, Information Warfare, Strategic Communication, Soft/Sharp Power, and Cyber Warfare give an idea of why Russia focuses on non-kinetic tactics, as well as conventional power, with the focus on influence, deterrence, and strategic advantage. It is argued that, according to the findings, the contemporary conflicts are more and more based on these combined, multidimensional strategies, and not on the traditional military force alone (Johnson, 2018). Also, the discussion throws light on the significance of international awareness, coordination of policies and resilience-building actions that states can undertake in order to reduce the effects of such hybrid threats. Altogether, this paper highlights that the knowledge of hybrid and informational tactics of Russia is the key to successful policy countermeasures and preserving global security (Mumford, 2017).

Realism (Neo-Realism and Classical)

One of the theories forming the basic aspect of international relations is realism, which focuses on power, national concern and survival in an anarchic international system where there is no common authority to implement rules. According to the classical realism theory advanced by Hans Morgenthau and other theorists, the states are naturally power-seeking actors that are motivated by human nature, ambition, and security need (Galeotti, 2018). Neo-realism or

structural realism is more concerned with the distribution of power in the international system and it implies that the actions of the states are influenced, to large extent, by the structural restraints, i.e., alliances, military capabilities, and relative power of other states (Hoffman, 2009).

Realism in the context of the Russian foreign policy offers a necessary paradigm in the way of interpreting the origins of the hybrid warfare and information operations utilization. Russia has suffered an extreme loss of military, economic, and political influence after the breakdown of the Soviet Union (Bettina, 2016). At the same time, the enlargement of NATO in the east and the political dominance of the West in the former Soviet countries developed the feeling of weakness and a tactical danger. According to realism, a state in such a situation is likely to seek every possible channel of achieving its interests as well as maximizing its security as well as recuperating its influence. Hybrid warfare is an idea of combining Russian military, economic, cyber, and information campaigns to demonstrate power without fully warring with other countries. This direction of Russia is logical, and this way, the country will be able to demonstrate its power without the need to enter the state of open warfare (Thornton, 2015).

One of the main aspects of hybrid warfare which is aligned with realist assumptions is information operations, which allow Russia to sabotage the unity, decision-making, and confidence of the opposing states, which increases the relative power position of Russia (Mansoor, 2012). As an illustration, in the case of the wars in Ukraine and meddling with the elections in Western countries, Russia engaged in the use of propaganda and disinformation campaigns to make the opponents politically and socially weak, which would give good opportunities to achieve its geopolitical interests. The concept of realism therefore interprets such indirect and non-military strategies as the instruments of state survival and power in a competitive and anarchic environment in international relations. The interpretation of hybrid warfare and information operations can be seen through realist prism by understanding the actions of Russia in terms of calculated actions to recover its position in the world and the balance with western primacy with minimum direct confrontation (Margaret, 2007).

Hybrid Warfare Theory (Gerasimov Doctrine)

The Hybrid Warfare Theory, which is a close companion to the works of the Russian General Valery Gerasimov, lays stress on an amalgamation of the military and non-military tools to accomplish strategic goals (Jonsson, 2019). Compared to the traditional warfare, the hybrid warfare incorporates the traditional kinetic force with the cyber operations, information campaigns, political influence, economic leverage, and irregular tactics. The gray zone of conflict is one of its major principles, as the actions are not clear enough to cause a direct retaliation or attribution, but they work well to produce strategic effects (Russell, 2009).

The example of this doctrine can be found in the way Russia goes about hybrid warfare. Russia put together unmarked soldiers, support of local militias, cyberattacks and synchronized propaganda campaigns in Crimea (2014) as well as Eastern Ukraine to destabilize the Ukrainian government and consolidate control over the territory (Bousquet, 2017). Russia was able to pursue its strategic objectives without having an open military confrontation with NATO because

it acted below the threshold of open warfare. The Hybrid Warfare Theory is focused on the flexibility and accuracy; states design operations to take advantage of particular vulnerability in target nations, which could be political polarization, social division, poor institutions, or economic dependence (Johnson, 2018).

The Eastern region is not the only part of the world where hybrid warfare is witnessed. In Syria, Russia backed Assad regime with its military action accompanied by much information campaign that described Russia as a stabilizer in the war on terrorism (Mumford, 2017). Hybrid approaches in the Middle East and Africa tend to combine use of private military organizations, undercover intelligence activities and influence in the media. The theory is useful in explaining why Russia spends on multidimensional capabilities that are a blend of soft and hard power, kinetic and non-kinetic actions to achieve foreign policy goals. This is why Hybrid Warfare Theory can give us conceptual background over the way Russia uses a variety of tools to obtain strategic results without conventional warfare (Galeotti, 2018).

Cyber Warfare Theory

The Cyber Warfare Theory is an analytical perspective of using digital technologies and digital networks to accomplish military, political, or strategic goals. Hacking, espionage, sabotage, manipulation of information and digital disruption are all under cyber operations (Hoffman, 2009). Cyber warfare is becoming a tool in modern conflicts, both as a part of a hybrid warfare strategy with traditional kinetic operations being supplemented by digital interventions and as a standalone tactic itself (Bettina, 2016).

Russia is now an international leader in cyber activities, using advanced technologies to attack critical infrastructure, government systems, political institutions, networks in the private sector, and social media (Thornton, 2015). Cyberattacks can be used in several ways: to interfere with the work of opponents, steal valuable information, promote disinformation, and impose psychological and political pressure. To illustrate, Russian cyberattacks on power systems and government systems have created massive disruption in Ukraine and cyber actions have been associated with election interference and leaking sensitive political information in the Western world (Mansoor, 2012).

Furthermore, Cyber warfare provides benefits to Hybrid warfare enabling the States to carry out actions in the 'Underground' subrange of the spectrum of warfare, with a strategic purpose. It makes it difficult to define the attributes and can also benefit actors who may be employing such tactics as Russia does to “wash the sanctions”, though with fewer potential retaliation consequences (Thornton, 2015). Cyber operations are frequently orchestrated in conjunction with information warfare, in which hacked information may be selectively released or fooled to shape and sway opinion in order to help sow the seeds for domestic political upset.

The process of embedding cyber tools within strategic communication portfolios, and the deployment and coordination process, is telling about the new approach that has been taken towards this. It is revealing to how Cyber tools have been embedded into strategic

communication portfolios, and deployed and coordinated (Russell, 2009). Also, cyber warfare offers a better way to engage in cross-border influencing operations not only because they are less expensive, but also because they are more scalable. Conducted remotely, the cyberattacks have more advantage of accessibility, efficiency, as opposed as the traditional military ones require a smaller number of physical resources. Russia has demonstrated that they can increase the complexity of malware, do them by phishing and use networks of disinformation which have been created to go against democratic systems and divide society (Jonsson, 2019). These operations are not only directed at the state but also on weaknesses in the civil society, media and electoral processes. In addition, as digital systems are becoming more and more reliant on digital infrastructure, the impact of cyber warfare has also been enhanced. The energy, financial, transport and communication systems are all vital areas that are highly vulnerable to cyber-attacks.

They can help these sectors to inflict economic instability, fear on the masses, and ultimately distrust among the population towards the government upon the attack. As a result, cyber warfare has become an integral part of a nation's national security plans. Cyber Warfare Theory shows, in very general terms, the growing importance of cyber domain in conflict in the modern era (Hoffman, 2009). It highlights the importance of enhanced cybersecurity regulations, global collaboration and strategic vigilance in combating the constantly-changing cyber threats. An understanding of these dynamics is essential for those making the type of policies and decisions that are crucial for securing the nation's interests and contributing to stability in the world.

Conclusion

To sum up, the analysis shows that hybrid warfare and information operations play the core role in the Russian foreign policy and enable the nation to accomplish strategic goals, control other states, and undermine opponents without involving military actions. Russia is successfully able to integrate military, cyber, political, economic, and informational means of operation in a manner that is coordinated and is operating in the gray zone between war and peace. The practicality and effectiveness of these strategies are evidenced by case studies of the Crimea, the Eastern Ukraine, the Syrian and the Western interference of elections. The research also demonstrates that the strategy of Russia is systematic, adaptive, and is informed with theoretical paradigms like: Realism, Hybrid Warfare Theory, Information Warfare, Strategic Communication and Soft/Sharp Power. The use of information and cyber activities intensifies hybrid tactics, develops perception, brings confusion and gains strategic benefits. In general, the study finds that the knowledge of hybrid and information activities in Russia is crucial to policy makers, scholars, and other international players in order to adequately address the current challenges of geopolitics and maintain stability in world politics.

Recommendations

- States at risk of Russian hybrid approach are supposed to enhance their cybersecurity systems, intelligence collection and counter-propaganda weapon much better to counter the attack of the cyber-attacks and disinformation programs.

- The governments are encouraged to promote educational campaigns and social efforts that assist individuals in identifying fake news, learning to discern manipulative stories, and developing resiliency to false information on the Internet.

- The strong collaboration among the countries allied with each other in terms of sharing information, strategies, and even diplomatic relations targeting the prevention of the hostile actions cannot be effective without close coordination.

- The states should have clear policies and mechanisms to identify, discourage, and react to ambiguous or covert activities that do not amount to open conflict.

- Continued studies of emerging hybrid approaches, as well as active communication efforts to combat fake news and misinformation and spread truthful facts will make national security policies dynamic and efficient.

Limitations

- The primary source used in the study is secondary data because it is hard to access classified or internal documents of the Russian government.

- Some sources, particularly those found in the media, might be biased or incomplete which influences the information accuracy.

- Hybrid warfare and information operations are dynamic and it is hard to encompass all the developments in recent past.

- The study concentrates on some case studies (Crimea, Eastern Ukraine, Syria, Western electoral intervention) that are not exhaustive on the issue of Russian strategy.

- Theoretical frameworks offer good analysis but they might not be adequate to explain the complex and adaptive nature of modern hybrid operation.

- Notwithstanding the drawbacks, the paper provides a detailed insight into the hybrid and

- information policy in foreign policy by Russia.

References

Ali, Abbas, H. (2005). *Pakistan's Drift into Extremism* (Vol. 2). New York: M.E. Sharpe.

Armstrong, K. (2000). *Islam: A Short History* . New York: Modern Library.

Bettina. (2016). Russia and 'hybrid warfare'. *Contemporary Politics, 22*(3), 283–300.

Bousquet, A. (2017). The battlefield is dead, long live the battlefield: Postmodern war and peace. *Journal of Strategic Studies, 40*(1), 1–27.

Christopher. (2017). Understanding Russian "hybrid warfare". *RAND Perspective, 233*, 1–12.

Galeotti, M. (2018). The mythical 'Gerasimov Doctrine' . *Critical Studies on Security, 6*(2), 157–161.

Hoffman. (2009). Hybrid warfare and challenges. *Joint Force Quarterly, 52*(1), 34–39.

Johnson, R. (2018). Hybrid war and its countermeasures . *Parameters, 48* (1), 5–16.

Jonsson. (2019). The Russian understanding of war: Blurring the lines between war and peace. *Journal of Slavic Military Studies, 32*(2), 1–18.

Mansoor, P. R. (2012). Hybrid warfare in history . *Cambridge Review of International Affairs, 25*(2), 1–15.

Margaret. (2007). Hybrid war: A new paradigm. *Military Review, 87*(4), 12–23.

Mumford, A. (2017). Hybrid warfare: The continuation of ambiguity by other means . *European Journal of International Security, 2*(3), 1–17.

Russell. (2009). Thoughts on hybrid conflict. *Small Wars Journal, 9*(1), 1–10.

Thornton, R. (2015). The changing nature of modern warfare . *RUSI Journal, 160*(4), 40–48.