Analysing Hybrid Warfare And Information/Cyber Operations

Nazish Mahmood, Ahmed Ijaz Malik, Muhammad Nadeem Mirza

Webology (ISSN: 1735-188X)
Volume 18, Number 4, 2021

Analysing Hybrid Warfare And Information/Cyber Operations

Nazish Mahmood[1] , Ahmed Ijaz Malik[2] , Muhammad Nadeem Mirza[3]

[1]Faculty Member School of Politics and International Relations Quaid-i-Azam University Islamabad

[2]Faculty Member School of Politics and International Relations Quaid-i-Azam University Islamabad

[3]Faculty Member School of Politics and International Relations Quaid-i-Azam University Islamabad , ORCID (https://orcid.org/0000-0002-2196-9174)

Abstract

The recent unclear thinking about war is predicated on entrenched theoretical concepts with limited understanding. This article aims to lead discussion on key terms being employed in the twenty-first century warfare like 'hybrid war', 'insurgency ', 'grey zone' operations, and the like. It also endeavours to explain the practical manifestations of the concepts like 4G / 5G warfare and its repercussions for countries like Pakistan. Empirically this study analyses that how the states and non-state actors have made effective utilisation of the cyberspace in order to launch attacks against the adversaries.

Keywords: Hybrid warfare, Grey Zone Conflict, 5th Generation War, Information/Cyber Operations, Propaganda.

Introduction

Proponents of hybrid war claim it as one of the novel ways being sought by both the state and the non-state actors in the contemporary global security landscape to achieve or maintain dominance, exercise influence over adversaries and realize self-interested outcomes at regional and global level. They maintain that contemporary global environment is particularly amenable to tools and techniques of hybrid war because the alternative could be conventional annihilation or the risk of nuclear escalation. Hybrid war actors are enabled by the processes of interconnectedness and the proliferation of technologies. Tools of hybrid war, hence, give states a way to operate outside the global norms on the use of force. The term though in vogue for more than a decade by the American military experts, ambiguity still exists as per its definition within the official circles.

The 'hybrid' in hybrid warfare refers to the state and non-state actors employing coordinated use of conventional military weapons save weapons of mass destruction (WMD). Irregular tools of warfare that traditionally include terrorism, insurgency, guerrilla warfare, criminal activity and disruptive technologies like hostile attacks on information technology infrastructure are all categorised as instruments of hybrid war but are not limited to it. Its principle architect Colonel (retired) Frank G. Hoffman defines hybrid threat as 'Any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle space to obtain their political objectives' (F. G. Hoffman, 2009). Hybrid threat combines attributes of both regular warfare with the unregulated irregular forces in the form of militias, guerrillas and criminals, and can operate as either when deemed appropriate (Department of the Army, 2011).[1]

'Novel' approaches like use of proxies, unmarked soldiers, special operation forces and social media are being increasingly employed by the state actors to manipulate adversary's information and capitalize on their perceived vulnerabilities. Information operations which are most frequently employed in the hybrid warfare can be of various types. Electronic warfare and other related domains such as propaganda and information operations all fall within the domain of information warfare tools (Mirza et al., 2021). These operations are meant to induce emotions amenable to one's own interest and employ traditional tools of dropping leaflets on adversary populations to contemporary internet-based spread of 'fake news. In a nutshell hybrid warfare employs all the possible means available with the states in order to achieve its objectives (Babar & Mirza, 2020; Sloan, 2018).

As stated before a plethora of terminologies are in vogue which confuses the reader to distinguish one concept from another. Rather than 'hybrid warfare' a term more frequently employed by the American officials is 'local wars' where the main enemies are local militias, terrorist groups etc (Batyuk, 2017; Department Of The Army, 1992).[2]

Later, LIC definition underwent further change and instead the change. The term 'irregular warfare' has been used to describe Low-Intensity Conflict (LIC) which is 'a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s)' (CCA, 1992). Indirect approaches are preferred in irregular warfare though it may employ the full range of military capacities in order to erode an adversary's power and influence. Another distinction to be kept in mind is that of 'compound warfare' and hybrid threats. While in case of former both irregular and traditional forces usually operate in different theatres, in later case a greater degree of coordination or fusion within the same battlespace is seen. What makes them significantly different from compound war is that they work under the unity of command in order to achieve unity of effort for attainment of a political objective (Leslie, 2011).

US military experts started employing term 'hybrid warfare' to describe 'local wars' at the height of Iraq War. It was an explicit realization that US with all of its military and technological preponderance was still unable to realize it desired political goals. The term continued to be used in testimonies before Congress by the senior US officials in 2008 and 2009 to describe the methods used by US adversaries in Iraq and Afghanistan. However, hybrid war represents something distinct from both regular and irregular warfare (Isherwood, 2009; Wither, 2016).[3] For scholars like Tad A. Schnaufer tactical aspects of hybrid war like applying intense diplomatic pressure, exploiting national and cultural identities and differences, large-scale military exercises along borders, dominating access to key economic resources like oil and gas, and using internet to wage false information media campaign are only part of the larger subversive and indirect strategy to weaken the enemy and is better expressed through the label 'non-linear warfare' (Schnaufer, 2017). Michael Evans, however, argues those preparing for twenty-first century combat must be prepared to confront range of forms of conflict and be ready for era of warfare quite different from that of the recent past (Evans, 2014).

What makes hybrid war unique is the combination of at least two elements and the ambiguity that lies inherent in what is being combined. A distinction however is to be kept in mind here. There is a group of believers who see this combination only in military forms. It is important to know the actors, targets and goals of the hybrid war in order to differentiate it from the conventional and irregular warfare. While the conventional war is waged by states which aim to target adversary's military forces using conventional tools; in irregular warfare the 'traditional' irregular tools are used by the non-state actors to target primarily the adversary military forces but the civilians are more easily accessible targets. However, these conventional and 'traditional irregular' tools are used in a coordinated way in hybrid war by both state and the non-state actors.

It is to be remembered that state's employment of hybrid war tools is far more complex because accessible 'novel' tools like proxies to attain preferable outcomes. Besides elements of political warfare (military, intelligence, diplomatic, financial and other means) are more easily incorporated by state-led actors into the hybrid war. Goals of state and non-state actors differ even when both target adversary's armed forces and civilians. We all understand that at the strategic level, war occurs between the people and each side actually aims at winning at the 'hearts and minds' of the people, while simultaneously trying to erode the popular support of the other side. State actor can have self-defined objectives vis-à-vis an adversary while non-state actors usually wage these hybrid wars for secession or forestalling a state actor from intervening. Thus, both have state actors as explicit targets.

What makes hybrid war new in the contemporary environment is the way it is purposefully and substantially integrated in a holistic way by the waging parties. Otherwise regular and irregular elements have generally been part of the war theatre since ages (Kofman & Rojansky, 2015; LANOSZKA, 2016; Wither, 2016). When the Chechen fighters employed modern military

communications technology that usually is associated with state-actors along with their predominant guerrilla warfare tactics in 1990s; and Hezbollah used high-tech military weapons like anti-satellite weapons by blending it with their irregular tactics during 2006 Israel-Lebanon War – the term hybrid war was used to capture the novelty of tools engaged to stymie adversaries' objectives. Still in both aforementioned cases waging parties were the non-state actors. A leading figure on hybrid warfare Frank Hoffman, however, was the first to argue in 2007 that in future war state actors would blend conventional military capabilities with irregular tools like terrorism and cyber warfare (F. Hoffman, 2007). Still it was not before 2014 when Russia invaded Crimea that the term was officially used by NATO to describe Russian method (NATO, 2014) and then onwards the term hybrid war is increasingly being associated with the state behaviour. Irregular war is no longer a secondary war theatre in today's hybrid war (F. Hoffman, 2007). Besides access to new tools such precision weapons and advance military communication technologies and cyber-related activity such as usage of internet to conduct information operations through social media has just made contemporary hybrid war more impactful. Given this complexity, any labelling of insurgent or counterinsurgent is problematic, and it fails to grasp the hybrid nature of these conflicts as well as the multiplicity of actors involved.

Contemporary hybrid war waged by the states thus falls in the 'grey zone' between war and peace as states deliberately avoid crossing the threshold to open conventional warfare and prefer strategies that are non-attributable (Babar & Mirza, 2020) or as S. D. Bachmann and Hakan Gunneriusson says there is 'masquerade of deniability' (Bachmann & Gunneriusson, 2015). Short-of-war strategies in the 'Gray Zone' like proxy warfare, the fait accompli, and 'salami tactics' helps create sufficient ambiguity in the mind of state's adversary to forestall any conventional military response and thus might involve very limited actual combat or no combat at all. Thus, the hybrid war seems a product of the concept of 'asymmetric warfare'. It is also sometimes referred to as 'ambiguous warfare' because it is seen in essence as 'blurring' of the situation where it is unclear who is a combatant and who is not, thus whether a state of war exists. This also explains central role of cyberwar in hybrid conflicts as the insistence on non-attribution for keeping tensions below the conventional war threshold. This makes it very difficult for the aggrieved party to determine the perpetrators of cyber-attack. That's why cyberspace has been designated as 'the crux of future of hybrid war' by Lora Saalman (Saalman, 2016). Cyber domain in spite of levelling the playing field for the state and the non-state actors still provide an edge to the state. The substantial resources states can devote to capability development are unsurpassable by the non-state actors. In cyberspace the battlespace is open to both the opponents and supporters and hence their opinions can be moulded by the information operations.

Amicahi Magen cites three shifting trends that facilitated the emergence of hybrid war since the end of Cold War. First, not only the protagonists of war have changed but the units against which it is measured and evaluated as well. Second, the formation of dynamic alliances (formal/ informal) between non-Western states and non-state actors like Iran-Syria-Hezbollah-Hamas has added a

qualitative innovation to the nature of transnational alliances (Magen, 2011).[4] The last dimension is the hijacking of "ungoverned spaces" by non-Western states and their non-state actor allies. These spaces then become breeding grounds for conflict, especially non-state actors establish cross-border criminal 'shadow economies' and simultaneously cement internal chaos and may trigger cross-border armed conflicts too (Magen, 2011). Hybrid war has several academic antecedents and 4GW is just one of them that likewise employ diplomatic, economic, financial, informational, intelligence and legal tools and can said to be the tactical manifestation of hybrid warfare.

Up till 2014, the overwhelming hybrid war analysts' focus has been asymmetrical tactics of non-state or sub-state actors rather than their use by the states. Perpetrators of hybrid war cannot claim that they are employing a defensive strategy. It is very much an offensive military strategy where a long game is pursued in the space short of clear-cut military action to obtain cumulative tactical successes. They then add up to a strategic win where the changed facts on the ground are accepted as fail accompli and the costs to restore the pre-existing status-quo for the defender could be not only substantially high but also unprofitable. It is used in a systematic, subtle and refined way especially by the state actors and backed by official discourse that denies and supports it and thus avoid moves that would trigger international community's automatic, robust response. Hybrid war thus has become an effective tool in the hands of non-status quo powers whether local, regional or global and the unique ways it is waged signals its centrality for the foreseeable future.

Hybrid War in Contemporary Practice

Contrary to the belief that hybrid war emerged because of US dominance in conventional warfare and its technological dominance par excellence, the adversary waging hybrid war is not a stupid enemy. It's a 'smart man's' war for engaging a superior force unable to be deterred or defeated by conventional methods. It is neither a replacement for traditional conflicts. In the contemporary security environment both state and non-state actors are engaged in hybrid war and their motivations as well as tools employed differ significantly from each other. The study will discuss one state (Russia) and one non-state (Hezbollah case) in order to give an idea how those getting the blame for waging hybrid war are utilizing it to gain their strategic objectives. This will help us later in contrasting the situation prevalent in Pakistan and whether any similarities or conclusions could be drawn from cases analysed.

The case of Russia

The drivers of change in the Russian approach to the new military thinking were the changes in its vicinity through the 'colour revolutions' where countries in Moscow's traditional sphere of influence were being turned away from the Kremlin and replaced with governments with pro-Western orientations. The 2008 war with Georgia was also not a feat worth highlighting from

military point of view. Besides Russians have an enduring belief in their country's historical standing as a great power and have always sought a privileged status while they felt the West was constantly trying to sweep them into a corner (Lange-Ionatamišvili, 2014).[5] They also suspected Western capitals to have orchestrated 'colour revolutions' and were harbouring intentions to effect similar regime change in Russia too (Bruusgaard, 2014). With this in mind a series of reforms were initiated by the Russian President Vladimir Putin within those structures that could contribute not only to his own power in a 'power vertical' (Lange-Ionatamišvili, 2014; Monaghan, 2011; TMT, 2013; Whitmore, 2015)[6] society but to the Russian power on the international stage - including its military.

Russia has accused US of using political, economic and military support to selected groups, and using covert actions and information operations during 'colour revolutions'. Russia claims that the hybrid warfare is a not a Russian, but a western concept. It further alleges that the West is waging a hybrid war against Russia (Monaghan, 2015). Foreign Minister Sergey Lavrov has been vocal in highlighting US role in regime changes in states following policies not agreeable to Washington (Lavrov, 2014) and accused US of waging hybrid war against them (Author, 2015; Lavrov, 2014).[7]

From Russian point of view they have 'reverse-engineered' the concept of hybrid war by adopting and refining these techniques in its modern military operations (Bruusgaard, 2014) and the result has been a unique doctrine that combined different military and non-military approaches into one (Tsypkin, 2010).[8] At the heart of such integration is to induce effectiveness of state levers of power which are more effectual when employed in complete concert with each other as compared to when they are just the sum total of their parts. What goes to Russia's credit is the way it has refined and integrated these elements beyond Western variant.

Crimea was seized by Russia with quite an ease, something that Sun Tzu calls as the 'acme of skill'- subduing of the enemy without fighting. But behind this seizure has been Russia's successful and 'novel' employment of traditional military tools with non-conventional techniques on the 'battlefield'. The hybrid campaign against Ukraine started months before actual Russian forces were committed for Crimea (HC 755, 2014). With the aim to either passively persuade enemy's government, military and population to welcome Russian occupation or to convince them that opposing such a path could lead to disastrous consequences. The principal tool to engender these thoughts is the information warfare through which either a positive image is built, or fear inculcated in the adversary.

It is important to highlight here that Western 'information operations' are used as adjunct to their military plans while Russians reversed the role by assigning them 'primacy' over more

conventional military techniques. This has also changed the centre of gravity and now 'people's mind' has become the target rather than the direct destruction of the enemy (Babar & Mirza, 2020).

Thus, using information tools such as television, social media, websites etc. a vision of reality is created that suits military and political purposes of the party waging hybrid war. What is important is not the quality but the quantity of information being received by the target country as it is more likely an individual would be receiving a Russian version or one of a number of versions at least. Adding a conspiracy theory gains much greater traction and hence influence as it makes the news more interesting than the mundane information. Thus, through synchronous execution of messaging implemented through state-controlled media outlets; narratives are controlled and are converted into tools of information warfare.

An additional advantage that Russia had in case of Crimea - that the now-independent states were once part of the Soviet Union. They have significant number of ethnic Russians as well as Russian speakers whom Russian law labels as 'Compatriots Living Abroad' (Lange-Ionatamišvili, 2014) and thus come under the ambit of the protection of Mother Russia. On the one hand, these 'compatriot Russians' were used to instil 'soft loyalty' by appealing to cultural, linguistic and ideological links while on the other hand, fear of the host government's retaliation was inculcated in the target groups and hence, an appeal to the option of a joint future destiny was embedded. These local populations, be they Russian–speaking or not are targeted to protest against the governing authorities and for Moscow to use their subsequent clampdown as an excuse for setting up local vigilante squads (which may or may-not have Russian special forces in civilian clothes or unmasked soldiers) to provide 'protection'. The ultimate end-game comes when locals influenced through sustained information warfare campaign seek 'humanitarian intervention' and then end up in joining Russia through the ballot box by the ultimate manipulation of the local politics (Thornton, 2015).

The hybrid war that Russia fought in Crimea was thus a 'contactless war' which provided certain advantages to Kremlin. It was able to add a new piece of territory without resorting to direct military confrontation. The chief reliance on information campaigns kept enemy at arm's length without the need to engage directly with adversary's 'hard military power'. Thus, it achieved the twin objective of minimum financial and human costs as well as blurring the lines to an extent where overt intervention by the Western States (having conventional military technological advantage on Russia) could be precluded. This aspect of 'plausibly deniable' also helped Moscow cultivate friends in the wider international community. Russia's asymmetric thinking and its information-warfare 'blitzkrieg' with forceful synchronized messaging was difficult for West with the free media to compete.

Hezbollah and Hamas

When the Israeli Defence Forces (IDF) suffered against the nominally weaker Hezbollah in the 2006 Second Lebanon War, the term 'hybrid war' surfaced to describe Hezbollah's fusion of

several distinct modes of war. In spite of Israeli air campaign lasting weeks and later ground invasion, Hezbollah using a combination of conventional tactics, modern high-tech weapons including strategic rocket assaults, unmanned aerial vehicles, night vision technology, improvised explosive device (IEDs), combined with small-unit movement continued to launch missiles into northern Israel making them struggle with targeting and force protection. Hezbollah's ceaseless attacks and strategic adaptation made Israel retreat. It had to confront another hybrid foe in the form of Hamas in the Gaza Strip in December 2008-January 2009 in Operation Cast Lead and again in July-August 2014 in Operation Protective Edge. The document 'IDF Strategy' released to public on August 13, 2015, labelled both Hezbollah and Hamas as hybrid foes and analysed threat posed by them that 'is constantly growing in volume, pace, range, accuracy, payload, and survivability. In addition, [the document stated] sophisticated military capabilities could undermine the IDF's offensive capacity in the ground, air, and sea theaters' (Herzog, 2015).

The history of the Arab-Israel conflict can also be read as a history of the shifting modes of war, from the conventional 'Clausewitzian War' of 1948, 1967, 1973 (fought by the regular forces, on defined battlefields for a defined period of time) to a clash between an assortment of non-state paramilitary organizations in the years 2000-2004. This qualitative shift in the nature of the Arab-Israel conflict occurred when groups like Hamas, Fatah and Islamic Jihad using suicide-attacks as a weapon of choice brought their struggle right into the hearts of Israeli cities under civilian garb and taking shelter among their own people. Tactics of war are embedded in the socio-political world in which they unfold, and they stem from institutional, legal, technological, and cultural conditions prevailing in the era. A group like Hezbollah evades labelling in the traditional sense because it simultaneously works as a political party, a conventional military force, a humanitarian organization and even as a state-sponsored terrorist group to some extent. Hence, Hezbollah using blend of multiple forms of combat ranging from conventional manoeuvre warfare to irregular tactics, information warfare, terrorist acts and criminal disorder embarrassed Israeli Defence Forces equipped with most modern technology in the Second Lebanon War (Biddle, 2008).[9]

Hezbollah massive involvement in the Syrian War gives it valuable experience in urban warfare that can then be replicated or quickly adapted against Israel (Chorev, 2016).[10] It is particularly difficult to eliminate the threat posed by these hybrid foes because wars waged by the adversary are non-linear, extended in time and space, and particularly 'nasty'. Psychological domain of the hybrid war seeks neither victory in the battle nor territorial gains, but the emphasis is in their psychological effect. Up till now both Hezbollah and Hamas have not only survived conventional superiority enjoyed by the IDF, but the hybrid war tools employed in their encounter has circumvented a humiliating defeat suffered by conventional Arab armies in previous full-scale Arab-Israel wars.

Conclusion: Hybrid War – Practical Manifestation of 4GW/5GW and its implication for Pakistan

Even those who otherwise question 4GW and 5GW constructs cannot deny a new form of warfare is emerging in the contemporary complex and dynamic environment. Increased global connectivity and scientific advances are giving way to global trends (competition for resources, proliferation and increased access of all forms of mass destruction etc.) that on the one hand are merging with local and regional tensions and increasing the frequency, intensity and extent of conflicts around the world; on the other hand, increased radicalism among marginalized communities is adding a dangerous dimension which is difficult to moderate or contain. Within such an environment weak and failing states or their likely collapse would contribute to sustained violence and bloody civil and sectarian wars. These weak adversaries are cognizant of their war-fighting capabilities and are determined to overcome their conventional disadvantage by adapting and exploiting vulnerabilities of their superior foes. Their access to information and advanced weaponry besides successful manipulation of kinetic and non-kinetic tools help them in successful realization of short and long-term objectives.

What makes hybrid wars particularly lethal in this context is that political element dominates this form of warfare, and they thrive on political communities that are constantly fed on fear and hatred towards each other and fighting for religious convictions, ideological, ethic or cultural reasons, or social discrimination. In the context of 5GW, the adversary will not restrict itself to the military realm but will attack the opponent from any of political, economic, social, cognitive, informational, cyberspace or airspace dimension. This multi-dimensional coordination among government, privatized or corporations for the control of a particular strategic entity will render the enemy helpless and extremely vulnerable. All of this point towards a more complex, dynamic, interconnected and volatile future cantering indigenous populations - their hearts and minds as the centre of gravity and outcome in this asymmetric conflict will be measured in terms of effects on the masses.

Pakistan and its security establishment has recently started utilizing more frequently terms such as ‘5GW’ and ‘hybrid war’ in their official lingo. Such usage highlights increased realization of a unique security environment that blunts conventional and outdated distinctions between kind of threats posed to its territorial integrity and sovereignty. It also portends a future that cannot be secured with a single approach to defence planning and demands radical re-evaluation of its existing national strategy, warfighting concepts and force-structure so as to make it compatible to combat future threats. Considering existing internal socio-economic problems, ethno-religious differences and other sensitive disputes prevalent in the country, a single untoward incident backed by a hybrid foe could trigger a chain of events that might leave its political and military leadership extremely vulnerable. Pakistan is a potentially complicated state and its structural vulnerabilities such as inter-ethnic relations, religious strife, poverty, bankruptcy, unemployment, political instability etc could make it an easy target for a hybrid foe. Hence, a detailed examination of the

phenomenon and the processes is required that might help to confront this ambiguous warfare being waged against it.

References

Author. (2015, February 12). Putin's war on the West. The Economist. https://www.economist.com/leaders/2015/02/12/putins-war-on-the-west

Babar, S. I., & Mirza, M. N. (2020). Indian Hybrid Warfare Strategy: Implications for Pakistan. Progressive Research Journal of Arts and Humanities, 2(1), 39–52.

Bachmann, S. D., & Gunneriusson, H. (2015). Russia's Hybrid Warfare in the East. Georgetown Journal of International Affairs.

Batyuk, V. I. (2017). The US Concept and Practice of Hybrid Warfare. Strategic Analysis, 41(5), 464–477. https://doi.org/10.1080/09700161.2017.1343235

Biddle, S. D. (2008). The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy. Strategic Studies Institute, U.S. Army War College.

Bruusgaard, K. V. (2014). Crimea and Russia's strategic overhaul. The US Army War College Quarterly: Parameters, 44(3), 10.

CCA. (1992). NCUACS 35/3/92, Section B Expeditions and Research. Churchill College Archives.

Chorev, M. (2016). 'Deterrence Campaigns' Lessons from IDF Operations in Gaza: Mideast Security and Policy Studies No. 115 (p. 65). The Begin-Sadat Center for Strategic Studies.

Department Of The Army. (1992). US Field Manual FM 7-98 No. 7-98. US Government. https://www.bits.de/NRANEU/others/amd-us-archive/fm7-98%2892%29.pdf

Department of the Army. (2011). United States Army Field Manual 3-0, Operations, Change 1. US Government, Washington, DC.

Evans, M. (2014). From Kadesh to Kandahar: Military theory and the future of war. In Strategic Studies (2nd ed.). Routledge.

HC 755. (2014). Towards the Next Defence and Security Review: Part Two – NATO: Ninth Special Report of Session 2014-2015. House of Commons Defence Committee.

Herzog, M. (2015). New IDF strategy goes public. The Washington Institute. Policywatch. https://www.washingtoninstitute.org/policy-analysis/view/new-idf-strategy-goes-public

Hoffman, F. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Center for Emerging Threats and Opportunities, Potomac Institute for Policy Studies. https://potomacinstitute.org/reports/19-reports/1163-conflict-in-the-21st-century-the-rise-of-hybrid-wars

Hoffman, F. G. (2009). Hybrid vs. Compound War, The Janus Choice: Defining Today's Multifaceted Conflict. Armed Forces Journal. http://armedforcesjournal.com/hybrid-vs-compound-war/

Isherwood, M. W. (2009). Airpower for Hybrid Warfare: Mitchell paper 3. Mitchell Institute for Airpower Studies.

Kofman, M., & Rojansky, M. (2015). A closer look at Russia's' hybrid war': Woodrow Wilson International Center for Scholars.

Lange-Ionatamišvili, E. (2014). Analysis of Russia's information campaign against Ukraine. StratCom-NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/analysis-of-russias-information-campaign-against-ukraine-executive-summary/150

LANOSZKA, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. International Affairs, 92(1), 175–195. https://doi.org/10.1111/1468-2346.12509

Lavrov, S. (2014). Remarks by Foreign Minister Sergey Lavrov at the XXII Assembly of the Council on Foreign And Defence Policy. Ministry of Foreign Affairs of Russian Federation. http://valdaiclub.com/a/highlights/remarks_by_foreign_minister_sergey_lavrov_at_the_xxii_assembly_of_the_council_on_foreign_and_defence/

Leslie, F. B. (2011). Twenty-First Century Warfare Will Be Hybrid. US Army War College, Carlisle Barracks, PA. https://apps.dtic.mil/sti/citations/ADA553122

Magen, A. (2011). Hybrid War and the "Gulliverization" of Israel. Israel Journal of Foreign Affairs, 5(1), 59–72. https://doi.org/10.1080/23739770.2011.11446443

Mirza, M. N., Ali, L. A., & Qaisrani, I. H. (2021). Conceptualising Cyber Sovereignty And Information Security: China's Image Of A Global Cyber Order. Webology, Volume 18(No. 5), 598–610.

Monaghan, A. (2011). The Russian Vertikal: The tandem, power and the elections. Russia and Eurasia Programme Paper: Chatham House, 1.

Monaghan, A. (2015). The'war'in Russia's' hybrid warfare'. The US Army War College Quarterly: Parameters, 45(4), 8.

NATO. (2014, July 1). Hybrid war—Hybrid response? NATO Review. https://www.nato.int/docu/review/articles/2014/07/01/hybrid-war-hybrid-response/index.html

Saalman, L. (2016). Little Grey Men: China and the Ukraine Crisis. Survival, 58(6), 135–156. https://doi.org/10.1080/00396338.2016.1257201

Schnaufer, T. A. (2017). Redefining Hybrid Warfare: Russia's Non-linear War against the West. Journal of Strategic Security, 10(1), 17–31.

Sloan, E. (2018, November 22). Hegemony, power, and hybrid war. Dialogue of Civilizations (DOC) Research Institute.

Thornton, R. (2015). The Changing Nature of Modern Warfare: Responding to Russian Information Warfare. The RUSI Journal, 160(4), 40–48. https://doi.org/10.1080/03071847.2015.1079047

TMT. (2013, May 21). Putin Strengthening Power Vertical, Report Says. The Moscow Times. https://www.themoscowtimes.com/2013/05/21/putin-strengthening-power-vertical-report-says-a24259

Tsypkin, M. (2010, February 27). What's New In Russia's New Military Doctrine? Radio Free Europe/Radio Liberty. https://www.rferl.org/a/Whats_New_In_Russias_New_Military_Doctrine/1970150.html

Whitmore, B. (2015, March 12). The Sick Man Of Moscow. Radio Free Europe/Radio Liberty. https://www.rferl.org/a/the-sick-man-of-moscow-putin-kadyrov-nemtsov/26898042.html

Wither, J. K. (2016). Making sense of hybrid warfare. Connections, 15(2), 73–87.