

Hybrid Warfare: Dynamics of Modern-Day Conflict

Fahim Tahsan¹

Hybrid warfare refers to the use of a combination of conventional, unconventional, and cyber warfare tactics by states and non-state actors to achieve their objectives. These tactics can include disinformation campaigns, cyber-attacks, and the use of proxy forces, among others. The COVID-19 pandemic has also been used as a tool of hybrid warfare by some countries. Due to the ever-changing nature of hybrid warfare, it is important to stay informed and aware of current events and developments to understand the current scenario. Additionally, hybrid warfare can be used as a tool for countries to assert their influence on the global stage without risking a direct military confrontation with a more powerful adversary.

There have been several examples of hybrid warfare throughout recent history. Some examples include the Russian annexation of Crimea in 2014, the ongoing conflict in Syria, the 2016 US Presidential Election, the ongoing conflict in Nagorno-Karabakh, cyber espionage and intellectual property theft by China for economic gain.

It is difficult to predict exactly when and where a hybrid war might occur in the future, as it can take many forms and be triggered by a variety of factors. However, there are a few potential flashpoints and scenarios that experts have identified as potential sources of future hybrid conflicts.

- **The Arctic:** As the Arctic region becomes more accessible due to melting ice, competition for resources and control of shipping lanes is likely to increase, potentially leading to a hybrid conflict among Arctic nations.
- **The South China Sea:** Tensions between China and other nations in the region over disputed islands and control of shipping lanes could potentially lead to a hybrid conflict.

¹ Fahim Tahsan is working as a Research Intern at the Bangladesh Institute of Peace and Security Studies. He has completed his Bachelor's in Disaster & Human Security Management from Bangladesh University of Professionals.

- **The Korean Peninsula:** The ongoing tensions between North and South Korea, as well as the potential for a collapse of the North Korean regime, could lead to a hybrid conflict.
- **The Middle East:** The ongoing conflicts in Syria and Yemen, as well as the potential for further instability in the region, could lead to a hybrid war.²
- **Cyber-space:** Cyber-attacks, both state-sponsored and non-state actors, are increasing in frequency and sophistication. A major cyber-attack on critical infrastructure could lead to a hybrid war scenario.³

It is important to note that these are just a few examples and the possibility of hybrid war could happen in any region of the world. Governments and international organizations must be prepared to respond to potential hybrid threats and continue to closely monitor potential flashpoints.⁴



² Wither, James, 'Making Sense of Hybrid Warfare', *Connections: The Quarterly Journal*, Vol. 15, No. 2, 2016, pp. 73-87; Monaghan, Andrew, 'The 'War' in Russia's 'Hybrid Warfare'', *Parameters*, Vol. 45, No.

³ Reisinger, Heidi and Aleksandr Golts, 'Russian Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence', *Research Paper*, No. 105, NATO Defence College, Rome, November 2014

⁴ Hoffman, Frank, *Conflict in the 21st Century: The Rise of Hybrid Warfare*, (Arlington: Potomac Institute for Policy Studies, 2007).

Tactics of Hybrid Warfare: Disinformation, Cyber-Attack, and Proxy Force⁵

Hybrid warfare tactics can be divided into three main categories: conventional, unconventional, and cyber. Some of the tactics that are commonly used in hybrid warfare include:

- **Disinformation campaign:** Actors use false and misleading information to manipulate public opinion and sow confusion and discord. This can include spreading fake news and propaganda, as well as manipulating social media platforms to influence public opinion.⁶
- **Cyberattack:** Actors use cyber means to disrupt, damage, or destroy the information systems, networks, and infrastructure of their adversaries. Cyberattacks can be used to steal sensitive information, disrupt critical services, and cause physical damage.
- **Use of proxy forces:** Actors use non-state actors such as militias or terrorist groups to carry out attacks or other actions on their behalf. This allows them to distance themselves from the actions of these groups and deny responsibility.
- **Economic warfare:** Actors use economic and financial measures such as sanctions, embargoes, and currency manipulation to weaken the target country and gain an advantage.
- **Psychological warfare:** Actors use psychological operations to influence the emotions, motives, objective reasoning, and behavior of the target country's population and government.
- **Political subversion:** Actors use covert or overt means to influence and subvert the political processes and institutions of the target country.
- **Military operations:** Actors use military force to achieve their objectives, such as occupying territory, capturing resources, or attacking military assets.

⁵ Winter 2015-16, pp. 65-74; Renz, Bettina, 'Russia and 'Hybrid Warfare'', Contemporary Politics, Vol. 22, No. 3, 2016, pp. 283-300.

⁶ Rácz, András, 'Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist', FIFA Report, No. 43, June 2015; Finnish Defence Research Agency (FDRA), 'On the Concept of Hybrid Warfare', Research Bulletin, No. 1, 2015; Cederberg, Aapo and Pasi Eronen, 'How Can Societies Be Defended against Hybrid Threats?', Strategic Security Analysis, No. 9, September 2015

- **The humanitarian crisis and social unrest:** Actors use non-conventional means to create a humanitarian crisis and social unrest in the target country to destabilize the government.

It's important to note that these tactics are not mutually exclusive and actors may use a combination of tactics to achieve their objectives.⁷



⁷ Cox, Dan, Bruscino, Thomas and Alex Ryan, 'Why Hybrid Warfare is Tactics Not Strategy: A Rejoinder to "Future Threats and Strategic Thinking"', Infinity Journal, Volume 2, Issue 2, Spring 2012, pp. 25-26.

Preventing Hybrid Warfare in 2023: Strategies and Solutions⁸

Stopping a hybrid war is a complex and difficult task, as it involves addressing multiple types of threats simultaneously. However, there are a few strategies that can be used to mitigate the risks and de-escalate a conflict⁹-

- **Diplomatic efforts:** Diplomatic efforts can be used to address the underlying issues that are driving a conflict and to build a coalition of nations to address the crisis.
- **Cyber defense:** Having robust cyber defense measures in place can help to mitigate the risks of cyberattacks, which are often a key component of hybrid warfare.
- **Countering disinformation and propaganda:** Disinformation and propaganda are often used as a tool in hybrid warfare, so it is important to counter false narratives and to promote transparency and accurate information.¹⁰
- **Strengthening international norms:** Strengthening international norms and institutions, such as the United Nations, can help to create a framework for addressing hybrid warfare and other types of unconventional conflict.
- **Building resilience:** Building resilience in critical infrastructure and communities can help them to withstand and recover from the impacts of a hybrid war.¹¹
- **Military response:** In some cases, a military response may be necessary to stop a hybrid war. However, it must be used as a last resort after diplomatic and other non-military options have been exhausted.

It is important to note that stopping a hybrid war requires a comprehensive and coordinated approach that involves all elements of national power, including diplomatic, economic,

⁸ 6 For example: Hunter, Eve and Piret Penik, 'The Challenges of Hybrid Warfare', International Centre for Defence and Security, Tallinn, April 2015; Maigre, Merle, 'Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO', Policy Brief, German Marshall Fund of the United States, February 2015; Berzins, Janis, 'Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense', Policy Paper, No. 2, National Defence Academy of Latvia, Centre for Security and Strategic Research, April 2014.

⁹ Aaronson, Michael, et al., 'NATO Countering the Hybrid Threat', Prism, Vol. 2, No. 4, 2011, p. 115.

¹⁰ Bachmann, Sascha-Dominik and Håkan Gunneriusson, 'Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security', Scientia Militaria, South African Journal of Military Studies, Vol. 43, No. 1, 2015, p. 79.

¹¹ North Atlantic Treaty Organisation, BI-SC Input to a NEW Capstone Concept for the Military Contribution to Countering Hybrid Threats, Brussels, 2010, pp. 2-3.

informational, military and intelligence. The international community should also be involved in this effort.



Hybrid Warfare in Strategic and Geopolitical Context¹²

Hybrid warfare fits into the broader strategic and geopolitical context in a number of ways. Some of the ways in which it can be integrated into a broader strategy include:

- **Achieving strategic objectives:** Actors may use hybrid warfare as a means to achieve broader strategic objectives, such as gaining control of resources or territory or projecting power and influence beyond their own borders.
- **Advancing geopolitical interests:** Actors may use hybrid warfare to advance their geopolitical interests, such as establishing or expanding spheres of influence, or discrediting or delegitimizing the target country or its institutions in the eyes of the international community.

¹² : 'Editor's Introduction: Complex Crises Call for Adaptable and Durable Capabilities', *The Military Balance*, Vol. 115, No. 1, 2015; Charap, Samuel, 'The Ghost of Hybrid War', *Survival*, Vol. 57, No. 6, December 2015–January 2016, pp. 51-58

- **Countering other actors:** Actors may use hybrid warfare as a means to counter the actions of other actors, such as by undermining the stability and security of a rival country or region.
- **Exploiting vulnerabilities:** Hybrid warfare can be used to exploit vulnerabilities in a target country or region, such as by capitalizing on social, economic, or political unrest to further their own interests.¹³
- **As a part of a larger conflict:** Hybrid warfare can be used as a part of a larger conflict, being a tool in the arsenal of the actors involved, as it can be used in conjunction with traditional military operations and other tactics to achieve their objectives.¹⁴
- **In response to changing global conditions:** Hybrid warfare may be used in response to changing global conditions, such as economic instability or shifting political alliances.
- **Long-term strategy:** Hybrid warfare can be used as a long-term strategy, taking place over many years and being integrated into the broader political, economic, and military objectives of the actors involved.¹⁵

Overall, hybrid warfare can be integrated into a broader strategic and geopolitical context as a means to achieve a range of objectives, counter other actors, and exploit vulnerabilities in a target country or region. Understanding the broader strategic and geopolitical context is crucial for understanding the motivations and objectives of actors involved in hybrid warfare, as well as for developing effective responses.¹⁶

¹³ Kofman, Michael and Matthew Rojansky, 'A Closer Look at Russia's "Hybrid War"', Kennan Cable, No. 7, April 2015; Neville, Seth, 'Russia and Hybrid Warfare: Identifying Critical Elements in Successful Applications of Hybrid Tactics', (Monterey: Naval Postgraduate School, 2015); Bartkowski, Maciej, 'Nonviolent Civilian Defense to Counter Russian Hybrid Warfare', The Johns Hopkins University Center for Advanced Governmental Studies, March 2015.

¹⁴ 'Research Publications', NATO Defence College, <http://www.ndc.nato.int/research/research.php?icode=0>, [accessed: 5 July 2017].

¹⁵ Iancu, Niculae, et. al, (eds), *Countering Hybrid Threats: Lessons Learned from Ukraine*, (Amsterdam: IOS Press, 2016).

¹⁶ Lasconjarias, Guillaume and Jeffrey Larsen, (eds), *NATO's Response to Hybrid Threats*, (Rome: NATO Defence College, 2015), p. XXVII.



Hybrid Warfare in Bangladesh: 2023 Scenario

It is not clear if there is a specific hybrid war scenario involving Bangladesh in 2023. It is important to note that predicting an exact scenario of a hybrid war is difficult as it depends on a number of factors and events that are not yet known.

However, it is possible that Bangladesh could be affected by regional tensions and conflicts that could potentially involve elements of hybrid warfare. For example, if tensions between India and Pakistan were to escalate, Bangladesh could be caught in the middle of a hybrid conflict. Additionally, as a country with a rapidly growing economy and a large population, Bangladesh could be a target for cyber-attacks or disinformation campaigns.¹⁷

It is important for the government of Bangladesh to be aware of the potential risks and to take steps to mitigate them. This could include building up its cyber defense capabilities, strengthening its institutions, and increasing its resilience to potential hybrid threats. Additionally, Bangladesh should also be engaged in regional and global efforts to address hybrid warfare, such as through the United Nations and other international organizations.

¹⁷ Joint Irregular Warfare Center, Irregular Adversaries and Hybrid Threats, An Assessment-2011, Norfolk, 2011

Lessons for the future: Recommendations from Ongoing Hybrid War¹⁸

There are several lessons that can be learned from the ongoing hybrid war and applied to prevent or mitigate future conflicts:

- **Early detection and response:** Early detection and response to hybrid warfare tactics, such as disinformation campaigns, cyberattacks, and the use of proxy forces, is crucial in order to prevent or mitigate their effects.¹⁹
- **Need for resilience:** Building resilience against hybrid warfare, such as strengthening civil society, democratic institutions, and critical infrastructure, can help to prevent or mitigate its effects.
- **Importance of international cooperation:** International cooperation is essential in order to effectively respond to hybrid warfare, as it allows countries and international organizations to share information and intelligence and to develop coordinated responses.
- **Need for comprehensive approach:** A comprehensive approach that includes diplomatic, economic, military, and information operations is needed to effectively respond to hybrid warfare.²⁰
- **Need for understanding the broader context:** Understanding the broader strategic and geopolitical context is crucial for understanding the motivations and objectives of actors involved in hybrid warfare, as well as for developing effective responses.
- **Importance of using an appropriate response:** Using an appropriate response, that is proportionate and tailored to the specific tactics and objectives of the actors involved, is essential in order to prevent or mitigate the effects of hybrid warfare.²¹

¹⁸ Renz, Bettina and Hanna Smith, (eds), 'After 'Hybrid Warfare', What Next? – Understanding and Responding to Contemporary Russia', Publications of the Government's analysis, assessment and research activities 44/2016, Helsinki, 2016, pp. 8-9.

¹⁹ Adamsky, Dima, 'Cross-Domain Coercion: The Current Russian Art of Strategy', Proliferation Papers, No. 54, November 2015, p. 21.

²⁰ Kofman, Michael, 'Russian Hybrid Warfare and Other Dark Arts', War on the Rocks, 11 March 2016, <https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/>, [accessed: 5 July 2017].

²¹ 5 Behnke, Andreas, NATO's Security Discourse after the Cold War, (London: Routledge, 2013), p.3

- **Need for transparency and accountability:** Promoting transparency and accountability in the use of hybrid warfare tactics can help to prevent or mitigate their effects, by exposing the actions of actors involved and holding them accountable for their actions.²²
- **Need for investing in critical infrastructure and emergency preparedness:** Investing in critical infrastructure and emergency preparedness can help to prevent or mitigate the effects of hybrid warfare, by making it more difficult for actors to disrupt critical services and by ensuring that the population is better able to withstand the effects of hybrid warfare.

It's important to note that the lessons learned may evolve over time as the situation changes and new information becomes available. It's also important to adapt the strategies and responses to the specific context, actors, and tactics involved.



²² Rynning, Sten, *NATO in Afghanistan: The Liberal Disconnect*, (Stanford: Stanford University Press, 2012), Behnke, *NATO's Security Discourse*, Chapter 10.

Conclusion

Hybrid warfare is a complex and evolving phenomenon that combines conventional military tactics with unconventional tactics such as cyberattacks, disinformation, and economic warfare. It can be triggered by a variety of factors and can take many forms. It's important to understand that predicting the future is uncertain and any potential scenarios can change rapidly. To effectively address and mitigate the risks of hybrid warfare, it is important for governments and international organizations to have a comprehensive and coordinated approach that involves all elements of national power, including diplomatic, economic, informational, military and intelligence. The international community should also be engaged in this effort.²³ It is also important to note that the term "hybrid war" is not a recognized term in the field of warfare, and it is unlikely that any country or group would be able to successfully conduct a hybrid war on a global scale. It is also important to note that hybrid warfare is not necessarily a successful war strategy as it can cause long-term damage to relationships and international order. The definition of success in hybrid warfare is also ambiguous. Finally, it is important to understand that preventing and resolving hybrid wars require a long-term, multidimensional and multilateral approach involving all actors, including civil society, private sector, international organizations and military. This approach should be focused on addressing the underlying causes of conflict, such as poverty, inequality and political repression, rather than just reacting to its symptoms.

²³ Samuel Charap, 'The Ghost of Hybrid War', *Survival*, Vol. 57(6), 2015/16, p. 52