RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 188 – 5 December 2024



# Finding Clarity in the Fog of Hybrid Warfare

*By Ian Li*

## SYNOPSIS

*Singapore's interest in hybrid warfare grew significantly following the Russian annexation of Crimea in 2014. Although the term has gained mainstream attention, there remains much ambiguity over its meaning. Several defining attributes in hybrid warfare can help shape response measures.*

## COMMENTARY

Hybrid warfare is a term that gained mainstream attention after Russia annexed Crimea in 2014. Following the recent cutting of two undersea fibre-optic communications cables in the Baltic Sea, Russia has once again been accused of waging hybrid warfare against the West. However, there is some confusion about what hybrid warfare means. Although the term is broadly understood in common usage, an ambiguity of detail has often led to it being used interchangeably with other terms and concepts, such as "grey zone conflict", i.e., coercive actions that occur below the threshold of war.

Unfortunately, for those seeking to understand hybrid warfare in its conventional application and finding ways to counter it, the broad spectrum of activities attributed to it is more a hindrance than an aid. Without clarity on how hybrid warfare should be defined, it is impossible to form any meaningful analysis of it. To better understand hybrid warfare, we would need to identify its defining attributes.

### An Evolving Concept

Hybrid warfare is not a monolithic term. It was first popularised in 2007 by Frank Hoffman, a retired US Marine Reserve infantry officer and former Pentagon analyst. Observing how Hezbollah was able to frustrate the Israeli Defense Forces (IDF) in the 2006 Lebanon War, Hoffman concluded that this was due to the synergies created

from the blending of Hezbollah's traditional irregular tactics with warfighting capabilities typically associated with state militaries, in this case, supplied by Iran.

Although Russia's actions during the annexation of Crimea have often been labelled as hybrid warfare by Western analysts, the term is not used by the Russians themselves. Instead, they operate under the framework of New Generation Warfare (NGW), which includes various activities that straddle the full spectrum of conflict. Nonetheless, what connects NGW to the broader discourse on hybrid warfare is its blending of multiple instruments, specifically non-military, to achieve objectives. To be sure, NGW does not eschew direct military action, but there is a greater emphasis on using non-military means.

It was the supposed impact of non-military tools such as information and cyber in the annexation of Crimea that inspired NATO's definition of hybrid warfare, which is described as an "effective and sometimes surprising mix of military and non-military, conventional and irregular components" and which can "include all kinds of instruments such as cyber and information operations". Over time, NATO's definition has been adjusted to place greater emphasis on the importance of subthreshold action within the grey zone over the use of conventional military force.

Given the term's amorphous nature, hybrid warfare does not have one single definitive interpretation. Instead, like cuisine, each country or actor's version has its own unique taste and flavour. Definitions will also continue to evolve over time. Therefore, it is important to consider the application of hybrid warfare in each specific context.

**Do Not Forget the Hybridity**

The most defining attribute of hybrid warfare is its hybridity. Hybrid strategies seek to combine various tools to create synergistic effects. For example, an information campaign might target a population's commitment to defence, indirectly hampering the military's ability to perform on the battlefield. To be sure, individual tools can be effective even when employed alone, but forgetting their synergistic potential can lead to a tendency to see the trees for the forest, losing sight of the broader strategic picture.

Of course, all war is hybrid to a certain extent, but what makes hybridity potent in modern hybrid warfare is how today's technology and global interconnectivity have allowed for unprecedented coordination between its tools in terms of speed, scale, and intensity. Social media, for example, has been transformative, enabling information narratives to reach a wider audience in a shorter timeframe than older communication methods.

A hybrid strategy is, therefore, limited only by its planner's creativity, and the wide range of available tools increases the permutations. Like eating a buffet, the hybrid actor can pick and choose the tools most suited to the task and combine them accordingly.

## Winning Without Fighting

It has often been said that hybrid warfare is about "winning without fighting". Indeed, many of the tools commonly associated with hybrid warfare tend to fall below the threshold of war, giving the impression that there is a lack of military application. While such a proposition is attractive, it obfuscates the severity of the threat.

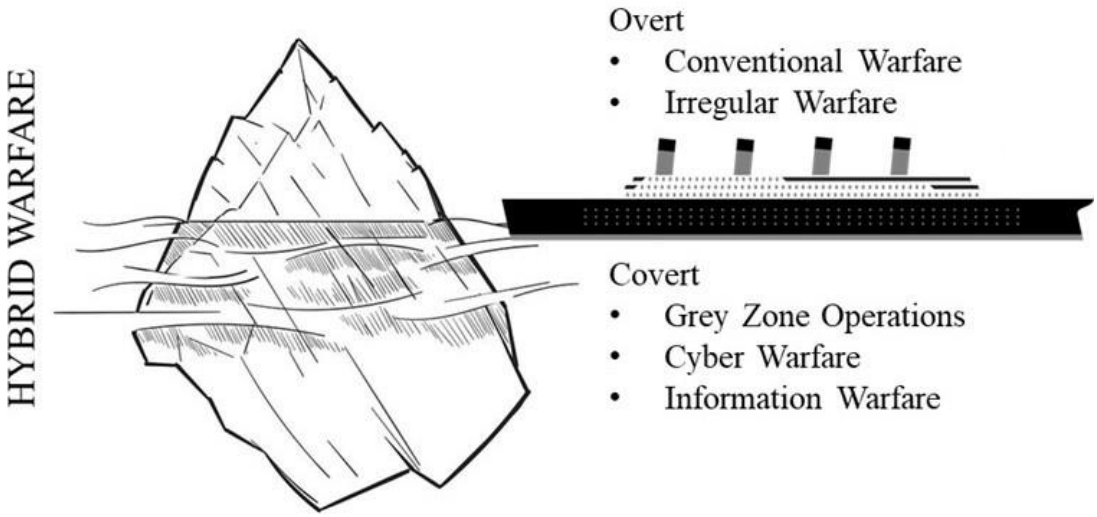
While hybrid warfare blurs the lines between war and peace, it is only because of how rigidly those lines are drawn. In Russian strategic thought, there is no distinction between war and peace, and thus, all actions have the potential to be militarised. Understanding intent is, therefore, key. If someone surveys a bank to plan for a future robbery, is it any less criminal than the act of robbing?

Furthermore, as the current Russia-Ukraine War shows, hybrid warfare does not preclude the use of conventional military force. If the hybrid warfare framework highlights the growing impact of non-military tools, it also reminds us that military force remains as relevant as a string to its bow. Forgetting this can potentially lead to the dangerous conclusion that the relevance of the military instrument has diminished in today's security environment.

If the military's footprint is less visible in hybrid strategies, it is by design and does not mean it is absent. Even in the annexation of Crimea, a large Russian force was deployed to the border to serve as a diversion and to intimidate Ukraine's leadership. The "war" in hybrid warfare reminds us that the military remains an essential backstop against hybrid threats.

## Building Resilience

Given the chameleonic nature of hybrid warfare, it is not always possible to recognise a hybrid campaign for what it is. In what is an "iceberg dilemma" (see figure below), the hybrid warfare iceberg is usually only recognised when impact nears and when more overt and decisive tools, such as the military, are finally brought to bear. This might still be preceded by a larger and more significant configuration of covert tools that go unnoticed because they operate beneath the surface within the ambiguous waters of the grey zone.




*The Hybrid Warfare "Iceberg Dilemma"*

Therefore, dealing with hybrid warfare is like treating a viral infection. Its components need to be dealt with aggressively and contained when encountered. However, a longer-term assurance for the nation's health requires building up immunities in areas where vulnerabilities are identified.

Singapore, for example, has adopted measures to strengthen its cyber and information resilience since 2014. To deal with cyber threats, the Cyber Security Agency was established in 2015, and the Singapore Armed Forces (SAF) Digital and Intelligence Service in 2022. Besides these, the Protection from Online Falsehoods and Manipulation Act and Foreign Interference (Countermeasures) Act were introduced in 2019 and 2021, respectively, to enhance the government's ability to respond to hostile information campaigns.

These agencies and legislations augment the strong and capable SAF, providing deterrence against military aggression and malicious actions, whether overt or covert. Illustrative of this was Ukraine's failure to contest Russia's annexation of Crimea, which was due more to its own military frailties than any brilliance in Russia's hybrid strategy.

Nonetheless, just as viruses constantly mutate, there is a need for constant monitoring for emerging vectors of threat and new vulnerabilities to develop the corresponding immunities. Furthermore, given the varied nature of the hybrid warfare toolkit, responses cannot just be based on a whole-of-government approach but whole-of-society.

*Ian Li is an Associate Research Fellow with the Military Studies Programme at the Institute of Defence and Strategic Studies (IDSS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.*