SEMINAR READ AHEAD

Dr Johann Schmid
Director COI Strategy & Defence
The European Centre of Excellence for Countering Hybrid Threats
johann.schmid@hybridcoe.fi

Hybrid Warfare – operating on multidomain Battlefields

This article builds on and further develops elements of Schmid, Johann (2019): COI S&D Conception Paper: Hybrid Warfare – a very short introduction (Helsinki, May 2019), ISBN: 978-952-7282-20-5

„War is more than a true chameleon that slightly adapts its characteristics to the given case." (Clausewitz (1832), On War, I, 1, p. 101).[1]

1 Clausewitz, Carl von. (1832/1980). Vom Kriege. Hinterlassenes Werk des Generals Carl von Clausewitz. Bonn: Dümmler.

"The very "rules of war" have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures -- applied in coordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces. (...)". Gerasimov, Valery Vasilyevich, Chief of the General Staff of the Russian Armed Forces, speech in front of Russian offices, February 2013.[2]

Hybrid warfare – a multidomain challenge for the EU, NATO and their member states[3]

Hybrid warfare of a type demonstrated, for example, on the Ukrainian battlefield, if carried out against European countries, would pose a particular challenge for Europe and the crisis management and defence of both NATO and the EU. Although it may seem unlikely from today's perspective, in an extreme case, NATO's military defence and deterrence posture could be bypassed by subversive means in a 'downward or horizontal escalation mode'. This may include possible threats (including military threats) from within, for example as a result of long-term subversion, infiltration, propaganda, destabilization or internal disintegration. Such hybrid threat- and attack-vectors may combine multiple domains and dimensions including e.g. politics, diplomacy, intelligence, media, information, economy, finance, infrastructure, technology, society, culture, law, psychology or morale - as elements of horizontal hybrid escalation. The military domain with its "operational sub-domains" - air, land, sea, cyberspace and space - being part of them. With their security and defence policy primarily oriented towards external threats, neither NATO nor the EU would be prepared, able or ostensibly entitled to protect their member states, as well as themselves as organizations, against such challenges at the blurred interfaces of war and peace, friend and foe, internal and external security as well as civil and military fields of responsibilities on multi-domain-battlefields.

At the same time, in a world of growing insecurity and global power shifts, dividing lines within EU and NATO and particularly within the societies of their member states are growing and deepening. Social and cultural tensions, radical ideologies, illegal migration, demographic

2 The speech was published in the'Military-Industrial Courier'(VPK), a Russian-language military specialist journal, on 27 February 2013: Cf.: Gerasimov, Valery Vasilyevich: 'Military-Industrial Courier' (VPK), 27 February 2013. The journalist Robert Coalson created a rough translation of the article in English and initially published it on his Facebook page on 21 June 2014 and later in the Huffington Post. Cf.: https://www. facebook.com/notes/robert-coalson/russian-military-doctrine-article-by-general-valery-gerasimov/10152184862563597. http://vpk-news.ru/ sites/default/files/pdf/VPK_08_476.pdf.

3 This chapter builds on and further develops Schmid, Johann (2019), 'The hybrid face of warfare in the 21st century'. Maanpuolustus, #127, 8 March 2019, Helsinki (FIN).

transformation, eroding respect towards state authorities, organized crime and on top the insecurity created by the current COVID-19 crisis situation function as catalysts in convergence of hybrid risk factors. They create additional lines of conflict and thus provide additional starting points for multidomain hybrid shadow-operations. This exposes numerous vulnerabilities on multiple domains that can be exploited by all kinds of hybrid actors - internal and external, state as well as non-state - from various directions, not only or primarily from Russia. However, military strength provides additional opportunities to exploit hybrid methods, even without the active use of force. Military escalation potential or dominance by its mere existence would therefore support any kind of subversive or horizontal hybrid activities on non-military domains.

In this context it has to be highlighted that losing the technological edge would create a severe risk for EU, NATO and their member states. As their military strength and defensive posture builds to a large degree on technological superiority, losing this advantage could create a "solidarity gap" for the collective defence of Europe as it would increase the risk and "price" of transatlantic engagement. As a result, European nations could be threatened by hybrid methods of warfare with growing credibility. For this reason, it is not promising that on certain technological fields, like on the field of electronic warfare, actors like Russia seem to be already way ahead of "western" capabilities. The same counts for the use of drones, which already proved to be a highly effective and efficient weapons system on various hybrid battlefields from Ukraine to Libya. Substantial drone and counter-drone warfare capabilities are still lacking behind in many EU-European nations.

However, success in hybrid warfare depends on certain preconditions that don't automatically apply to any situation. For example, the Crimea scenario (2014) could not be implemented elsewhere in offhand manner. The war in Donbas already demonstrated the limitations of such an approach.

The Ukraine case, however, illustrates another important relationship.[4] The more closely connected and interwoven a country's relations with its adversary, and the more pronounced their mutual dependencies on multiple domains, the more potential starting points there are for hybrid methods of warfare, which will also tend to be more successful as a consequence. For this reason, globalization, close international interaction and interconnected societies – as positive and desirable as these developments may be – have the potential to open up additional starting points for multidomain hybrid methods of warfare. This could make hybrid warfare a particularly favoured means among former (alleged) friends (as Ukraine and Russia had been), within the framework of intrastate conflicts, and especially in civil wars. Open, democratic societies that lack strategic vigilance are particularly vulnerable to such hybrid methods of warfare.

4 Cf. Schmid, Johann (2019): Hybrid warfare on the Ukrainian battlefield: developing theory based on empirical evidence. In: Sciendo: Journal on Baltic Security, Tartu August 2019; 5(1): (p. 5-15), ISSN: 2382-9230. http://www.degruyter.com/view/j/jobs.2019.5.issue-1/jobs-2019-0001/jobs-2019-0001.xml

Conceptualization of Hybrid Warfare in a Nutshell

Hybrid warfare is a specific style of warfare and strategic in nature. It makes use of multiple military as well as non-military domains and combines the tailored use of hard, soft and smart power elements with symmetric as well as asymmetric means and methods. Hybrid warfare is war potentially including all levels of escalation from subversion and destabilisation to the use of military force in all its possible manifestations. Hybrid warfare in the narrower sense (as all war is hybrid) and in contrast to its' counterpart – military centric warfare[5] -, can be described by three key characteristics and their hybrid orchestration. These elements form a threefold Hybridity:

1. **Field of decision:** Hybrid warfare involves a broad spectrum of domains and dimensions including all potential sources of power. Despite its use of force component however, hybrid warfare flexibly focuses the decision of a confrontation as such primarily on multiple and potentially shifting non-military centres of gravity. These include e.g. political will, economy, technology, information, society, culture, psychology, legitimacy or morale.

2. **Conduct of operations:** Hybrid warfare tends to particularly exploit vulnerabilities in the grey areas of interfaces. Therefore, hybrid warfare actors tend to operate simultaneously on multiple domains in the shadows/grey areas of various interfaces: E.g. between war-peace, friend-foe, internal-external security, civil-military domains, state-non-state actors, virtual-real world, reality-propaganda. By doing so, hybrid warfare blurs traditional lines of order and responsibilities while aiming for their subsequent dissolution. Thus, hybrid warfare creates ambiguities and makes attribution difficult in order to paralyze the decision-making process of an opponent while limiting his options to respond. At the same time the approach heads at avoiding, to be confronted with the opponents' strengths.

3. **Employment of means and methods:** Hybrid warfare creatively combines and makes parallel use of different civil and military, regular as well as irregular, symmetric and asymmetric, open and covert, legal as well as illegal means and methods, tactics, strategies and concepts of warfare. It creates ever new mixed hybrid forms designed and tailored to hit at vulnerable interfaces by employing multi-vector attacks.

5 To be understood as the form of warfare with its centre of gravity primarily focused on an overall military decision of a war/conflict and with a military decision on the battlefield being able to decide the entire conflict/war. E.g. along the lines of big portions of the Napoleonic Wars or both world wars. A bias in such thinking makes it at the same time more difficult to understand the specific logic of hybrid forms of warfare. Cf. Schmid, Johann: Der Archetypus hybrider Kriegführung. Hybride Kriegführung vs. militärisch zentrierte Kriegführung. In: Österreichische Militärische Zeitschrift (ÖMZ), Heft 5/2020 (in the publishing process).

While hybrid warfare actors generally resort to creative and indirect strategies of limited warfare and a limited use of military force, it must be emphasized that hybrid warfare potentially includes all levels of escalation. Friction and uncertainty are always part of the game and the perceived manageable use of force may get out of control. Due to its focus on a broad spectrum of non-military domains and centres of gravity, however, a military decision as such is not necessarily required for hybrid warfare actors to achieve their political goals. As happened in Donbas or during the Second Indochina War[6], militarily it may be sufficient for the hybrid warfare actor to prevent his opponent from deciding the war on the military battlefield, while seeking a decision himself on a non-military centre of gravity. Morale and legitimacy can become strong weapons in this context.

6 Cf. Schmid, Johann (2017), 'Hybride Kriegführung in Vietnam – Strategie und das center of gravity der Entscheidung'. In: Zeitschrift für Außen- und Sicherheitspolitik (ZFAS), Vol. 10, No. 3, Wiesbaden, 373–390. DOI: 10.1007/s12399-017-0659-4.

Outlook: Danger of offensive options - need for comprehensive understanding[7]

Hybrid warfare is a strategic concept which, if used offensively, could become a game changer for Europe's - EU, NATO, member states - security and defence. It particularly challenges the interfaces between war and peace, friend and foe, internal and external security, state and non-state actors, civil and military domains as well as between regular and irregular means and methods on multiple domains.[8]

As demonstrated on the Ukrainian battlefield, for example, or by the so-called Islamic State in Syria and Iraq in a different empirical manifestation, hybrid forms of warfare are conducted on interconnected multidomain battlefields: From the battlefield of ideas and ideologies and the fight for the "hearts and minds" of the people to the field of economic and financial pressure, from the diplomatic parquet to the military battlefield, not forgetting about the competitive spaces of information, law, technology, norms, values and psychological sentiment and many more. Hybrid methods of warfare appear to offer unpretentious political success by smart recourse to a limited, deniable and supposedly manageable use of force. Today hybrid warfare is particularly empowered by globalization and new technologies as catalysts. Technological trends such as artificial intelligence, quantum sciences, 5G technology, space assets, autonomous systems, cyber capabilities, extended reality or ubiquitous sensors open up new avenues for hybrid action in the grey zones of interfaces between various domains and dimensions.[9] The insecurity created by the current COVID-19 crisis situation in addition improves the starting conditions for hybrid action. The assumption that the risk of military escalation and political damage could be kept within limits in hybrid warfare may at the same time increase the likelihood of its offensive use. For this reason, it is more than likely that multidomain hybrid warfare in its various manifestations will shape the 'face of war' in the 21st century.

---

7 This chapter builds on Schmid, Johann: COI S&D Inspiration Paper, The hybrid face of warfare, ISBN: 978-952-7282-17-5, Helsinki, March 2019.

8 Cf. Schmid, Johann (2019), ´The hybrid face of warfare in the 21st century'. Maanpuolustus, #127, 8 March 2019, Helsinki (FIN).

9 Cf. Thiele, Ralph (2020), Artificial Intelligence – A Key Enabler of Hybrid Warfare, Hybrid CoE Working Paper 6, Helsinki, March 2020, ISBN 978-952-7282-31-1; Cf. Thiele, Ralph (2020), Quantum sciences – A disruptive innovation in hybrid warfare, Hybrid CoE Working Paper 7, Helsinki, March 2020, ISBN 978-952-7282-32-8.

Clearly, it offers offensive options in particular. However, the assumption that the use of force and the risk of escalation could be limited, and political damage manageable, might be misplaced, as uncertainties, friction and the tendency to go to extremes are essential characteristics of the nature of war. The combination of supposedly unpretentious political success and manageable risk makes hybrid warfare particularly dangerous. Moreover, by adopting a silent, covert and indirect approach that fosters ambiguity and makes attribution difficult, hybrid warfare actors may achieve their political goals and change the status quo of a given political situation inconspicuously (salami tactics), or unexpectedly by surprise (fait accompli) before the victim even realizes they are under hybrid attack. The current COVID-19 crisis situation provides additional opportunities in this regard as it increases global insecurity on multiple domains, from public health to politics, from the economy to society and finally to global power politics and geostrategic confrontation.

With this in mind, it is high time that the EU, NATO and their member states improved their common and comprehensive understanding of hybrid warfare as a multidomain strategic challenge simultaneously employed on multiple battlefields. Connecting respective dots on multiple domains with each other is therefore the only way to discover hybrid strategies. Indeed, such an understanding is a precondition for joint and comprehensive action in defence and response, as well as for deterring, preventing and containing the offensive use of hybrid warfare in the first place. Building the respective analytical capabilities, and educating the judgement of political leaders and decision-makers accordingly, would naturally be the first step in countering hybrid warfare. To develop a comprehensive understanding of hybrid warfare as a creative combination and dynamic integration of different battlefields on multiple - military as well as non-military - domains with shifting centres of gravity would be a most promising starting point in this regard.

Key messages:

- Hybrid Warfare is a creative combination of different battlefields on multiple domains by the dynamic use of multidomain operations and shifting centres of gravities.
- Therefore, hybrid warfare could also be described as “mosaic warfare” on interconnected multidomain battlefields.
- Empowered by globalization and new technologies and inspired by the “promise”/perception of unpretentious political success at supposedly manageable military risk and political cost, it can be expected, that the future of war to a large degree will be hybrid warfare.
- To counter hybrid warfare calls for a comprehensive hybrid answer on multiple domains including multidomain and cross-domain operations. Multidomain situational awareness would therefore be a necessary precondition.
- As hybrid warfare may include “conventional” combat at all stages of escalation against a militarily symmetric or even superior opponent, the EU, NATO and the member states must re-evaluate their conventional military warfare capabilities to provide national and collective defence, while at the same time protecting themselves against downward and horizontal escalation and threats from within, in the form of subversion, infiltration and disintegration on multidomain battlefields. It is paradoxical that the threat of hybrid warfare highlights, among other things, the necessity to re-establish substantial conventional warfare capabilities. [10]
- Countering hybrid warfare in addition requires the ability to protect vulnerable interfaces and to operate in the grey areas of multidomain battlefields by adopting a truly comprehensive approach. This includes a whole-of- government approach, a whole-of-nation/society approach, as well as international cooperation and coordination, particularly between and within EU and NATO. [11]
- Warfighting on multidomain hybrid battlefields is neither exclusively nor primarily a soldiers’ task. Hybrid Warfare is characterized by multiple and shifting centres of gravity while creatively making use of multi-vector attacks on various domains and dimensions. To counter hybrid warfare thus calls for a coordinated multidomain answer and includes a broad variety of relevant, civil as well as military, state as well as non-state actors.

10 Cf. Schmid, J., ´The hybrid face of warfare in the 21st century’. Maanpuolustus, #127, 8 March 2019, Helsinki (FIN).

11 Cf. Schmid, J., ´The hybrid face of warfare in the 21st century’. Maanpuolustus, #127, 8 March 2019, Helsinki (FIN).