Research Division
NATO Defense College

NATO@70

NDC POLICY BRIEF
No. 19 – September 2019

From hybrid warfare to "cybrid" campaigns: the new normal?

Antonio Missiroli *

The speed and intensity at which the strategic landscape has evolved over the past two decades requires constantly updating our analytical and operational tools, capturing change as it occurs, anticipating it whenever possible, and also framing it in terms that facilitate adaptation and cooperation. The recent debates over "hybrid" are an excellent case in point.

What's in a name?

The term "hybrid", as associated with "warfare", made its first appearance a decade ago among American military analysts. It was Frank Hoffman, in particular, who first coined it. He acknowledged that other definitions (such as "unrestricted", "compound" or "4th generation") had already captured the emerging features of 21st century warfare, as carried out by both state and non-state actors. Hoffman characterized "hybrid" as involving "a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder".[1] He based his empirical analysis on the tactics used by Hezbollah in the conflict with the Israeli Defence Forces (IDF) in South Lebanon in 2006, but the experience of the US with insurgents in Afghanistan and Iraq provided additional backdrop.

Hoffman articulated two interconnected terms: hybrid "war" proper, encompassing different modes of warfare in various possible combinations, and hybrid "threats", indicating the actor that employs them. For both, the emphasis was exclusively on operational *military* activities "directed and coordinated within the main battlespace to achieve synergistic effects". For Hoffman, the Hezbollah provided "the clearest example of a modern hybrid challenger", combining highly disciplined, well trained and properly equipped regular units, adaptive guerrilla tactics in both urban and mountainous areas, high tech weapons and UAVs, and swift and effective information operations, allowing it to take the IDF by surprise and forcing it into a military and political stalemate.

Written by and for the US top brass, this definition offered both strictly military orientation and conceptual practicality, and it opened the floodgates to a flurry of historical and empirical studies applying the "hybrid" label to more traditional cases of "asymmetric" warfare.[2] In retrospect, the main contribution of Hoffman's work was its emphasis on contemporary military technologies and Information and Communication Technologies (ICT) (what we now call "cyber") as having a multiplier and acceleration effect on those tactics. Interestingly, it also entered NATO's strategic discussions, mainly through the initiative of then Supreme Allied Commander Transformation, General James Mattis, who partnered with Hoffman in launching the concept in the first place.[3]

Subsequently, it was Russia's actions in Ukraine in

* Assistant Secretary-General, Emerging Security Challenges Division, NATO. The author writes in a personal capacity.

1 This and other references here are from F.G. Hoffman, *Conflict in the 21st century: the rise of hybrid warfare*, Potomac Institute for Policy Studies, Arlington, 2007.

2 See e.g. W. Murray and P.R. Mansoor (eds.), *Hybrid warfare: fighting complex opponents from the ancient world to the present*, Cambridge University Press, Cambridge, 2012.

3 J.N. Mattis and F.G. Hoffman, "Future warfare: the rise of hybrid wars", *Proceedings*, Vol.131, No.11, 2005, pp.18-19.

2014, building on the methods used against Georgia in 2008, which lent the term a new lease of life. However different in nature and scope, both the occupation and annexation of Crimea and the ensuing "rebellion" in the Donbas prompted a reconceptualization of "hybrid warfare" and catapulted it into the public debate. NATO's 2014 Wales Summit Declaration highlighted "the specific challenges posed by hybrid *warfare* threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design". In November 2015, the Allies agreed a dedicated "Strategy on NATO's Role in Countering Hybrid Warfare", while openly discussing its functional and geographical scope.[4] The Alliance's Warsaw Summit Communiqué (July 2016) spoke for the first time of "terrorist, cyber or hybrid *attacks*", potentially originating from all strategic directions, and indicated that NATO could respond to hybrid *warfare* by invoking Article 5 of the Washington Treaty. Two years later, the Alliance's Brussels Summit Declaration mentioned "hybrid *challenges*, including disinformation campaigns and malicious cyberattacks", and "hybrid *activities* that aim to create ambiguity and blur the lines between peace, crisis and conflict", confirming NATO's readiness to invoke Article 5 in the event of hybrid *warfare*.

Both the occupation and annexation of Crimea and the ensuing "rebellion" in the Donbas prompted a reconceptualization of "hybrid warfare"

The debate soon involved national security communities, especially in France (where it was linked to the domestic terrorist threat), the UK and Central Europe. For its part, the EU first established (April 2016) and then regularly reviewed a "Joint Framework on Countering Hybrid Threats", and agreed to cooperate closely with NATO – through two Joint Declarations (2016 and 2018) and a detailed list of actionable proposals.[5]

Comparisons were also drawn between Russia in Ukraine and ISIL/Daesh with its short-lived "Caliphate". Accordingly, ISIL's distinctive hybrid approach blended kinetic and information operations locally – in the Levant, including seizure of physical territory and practice of government as a "quasi-state" – with the instigation of terrorist activities globally. Last but not least, growing attention was paid to China's doctrine (and practice) of the so-called "three warfares" – psychological, public opinion, and legal – as articulated in a set of recommendations promulgated by the People's Liberation Army (PLA) in 2003. Though elaborated with special reference to Taiwan and the South and East China Seas, a number of experts saw them as inspiring Beijing's increasingly assertive behaviour on the international scene.[6]

The quick success of the concept was due, at least in part, to the intrinsically ambiguous nature of the term "hybrid" but also, in part, to the misuse of the terms "war" and "warfare". Russia's "little green men" in Crimea carried out a smart, swift and stealthy military and ICT operation that can indeed be characterized as "hybrid warfare", although it was "asymmetric" in reverse – so to speak – as Moscow was the stronger side on the ground. For their part, the alleged "rebels" in the Donbas constituted – in Hoffman's language – a truly hybrid "threat" to the Ukrainian military but Russia, as such, did not directly engage in "warfare" there. Ever since, hostile intelligence operations carried out by Moscow in the West – such as the Skripal assassination attempt or the failed hack of the Organization for the Prohibition of Chemical Weapons (OPCW) and World Anti-Doping Agency (WADA) networks – have often been labeled as "hybrid" and "war"-like.

In addition, Russia's overall aggressive conduct seemed to translate into operational reality what some analysts called the "Gerasimov doctrine", from Russia's then deputy Chief of military staff Valeriy Gerasimov's vision of "non-linear" (rather than "hybrid") warfare, as articulated in a series of articles published in 2013. On the other hand, Russian analysts did use an equivalent of the term "hybrid warfare" (*gibridnaya voina*) with reference to the way in which the West, and especially the US, had operated – through *non-military* means – both before and after the end of the Cold War to weaken Moscow. In particular, Russians saw the (in)famous "Colour Revolutions" in the post-Soviet space as direct results of that Western/American approach, later applied also to Yanukovych's Ukraine before the 2014 crisis.[7]

In other words, the semantic overstretch of the "hybrid warfare" concept contributed to a growing politicization of its use while, in fact, "hybrid" tactics were already shifting towards intelligence operations falling below the level of armed conflict and characterized by a higher degree of opacity and deniability.

4 G. Lasconjarias and J.A. Larsen (eds.), *NATO's response to hybrid threats*, NDC Forum Paper, No.24, Rome, 2015.

5 See D. Fiott and R. Parkes, "Protecting Europe: the EU's response to hybrid threats", *Chaillot Paper* No.151, EUISS, Paris, April 2019.

6 S. Lee, "China's 'three warfares': origins, applications, and organizations", *Journal of Strategic Studies*, Vol.37, No.2, 2014, pp.198-221.

7 M. Galeotti, *Hybrid war or* gibridnaya voina*? Getting Russia's non-linear military challenge right*, Mayak Intelligence, Prague, 2016. For a skeptical view see R.N. McDermott, "Does Russia have a Gerasimov doctrine?", *Parameters*, Vol.46, No.1, 2016, pp.97-105.

In military terms, it is fair to conclude that what has been labelled as "hybrid warfare" amounts to a new conceptualization of an already existent practice of blurring and blending different methods and tactics – but with additional emphasis on the way in which "cyber"-enabled technology works as a potential game-changer.[8]

Moving target(s)

Despite laudable efforts made, for instance, by the Multinational Capability Development Campaign (MCDC) or the new European Centre of Excellence in Helsinki, there is no agreed international definition of what a "hybrid" activity precisely is. Yet the fluidity of the concept is no reason to contest it, especially as it has now officially entered our political vocabulary: on the contrary, its inherent catch-all nature can be used as a prism to capture trends and phenomena that keep evolving and adapting. For instance, low-intensity hybrid operations may still constitute the beginning of something bigger that may in turn escalate to the level of "warfare". Yet it is equally clear that they often aim at simply testing and probing the other side's capabilities – by trial and error, by design or randomly, with a strategic or just opportunistic approach.

It is also evident that "cyber" is an essential vector – as a means and, occasionally, also an end – for all these operations. It is now both a military domain in its own right (alongside land, sea and air) and the "space" in which most of our economic, civilian and even personal activities unfold – a domain of domains, so to speak.[9] It is not by accident that one of the first tabletop exercises ever carried out at ministerial level in this area, organized during Estonia's EU presidency in 2017, was codenamed "CYBRID 2017", and that many similar ones have followed since, especially at NATO level. By using cyberspace, these operations tend to be – at least in comparative terms – low cost, low risk and high impact, and therefore quite accessible and rewarding. What is more, they do not know physical borders or respect territorial jurisdictions.

Despite the lack of an agreed definition, however, there is some broad common understanding of the nature of the threats and challenges we label as "hybrid". To qualify as such, these need to include coordinated and roughly simultaneous operations: in other words, not every single hostile and unconventional activity under the threshold of armed conflict is, per se, "hybrid". They also tend to be scalable, both horizontally (onto additional domains) and vertically (up or downwards). They tend to be targeted and tailored to specific vulnerabilities: every hybrid campaign is unique, although some common patterns are discernible. Finally, they tend to be hard to detect and hard to attribute, although some footprints are increasingly recognizable.[10]

Predictably, NATO tends to emphasise their potential links with military, paramilitary and intelligence activities, with a focus on their overall coercive effects. For its part, the EU tends to highlight their potential disruptive effects on the functioning of the single market and more recently also on the functionality of domestic political processes – since it has become apparent that sophisticated hybrid campaigns may have affected the integrity and even the outcome of democratic elections.

Such campaigns may employ different methods: focused "hack-and-leak" operations, large scale influence operations through social media and, at least in principle, vote manipulation – although the emphasis now is all on the "weaponisation" of social media.[11] Available evidence shows that these campaigns are most effective when they target "swing" electoral constituencies and when the choice at hand is binary (e.g. referenda) – less so, for instance, when some form of proportional representation is applied. However, after our "Sputnik moment" (when evidence of electoral interference in the US and elsewhere first emerged), our increased awareness of these risks has probably contributed to mitigating them – or diverting them elsewhere.

Traditional conflict prevention and arms control mechanisms seem difficult to apply to the "cybrid" domain

Perhaps most importantly, all the "hybrid" threats and campaigns outlined above are hard to deter and hard to respond to. To start with, they often belong in the domain of foreign intelligence operations as carried out by most states: such operations are not forbidden by international law, although they can be prosecuted domestically through law enforcement. Of course, things would change if/when espionage

8 See especially O. Friedman, *Russian "hybrid warfare": resurgence and politicisation*, Hurst & Co., London, 2018, which constitutes the most complete study on the concept to date.

9 For an overview see A. Missiroli, "The dark side of the Web: cyber as a threat", *European Foreign Affairs Review*, Vol.24, No.2, 2019, pp.135-152.

10 Attribution, be it private or public, involves technical, legal and political aspects. In the case of terrorist groups, which tend to "overclaim" rather than deny actions, the specific challenge is to verify their credibility.

11 P.W. Singer and E. Brooking, *Like war: the weaponisation of social media*, Mifflin Harcourt, Boston-New York, 2018. General David Petraeus once famously spoke, referring to insurgencies, of "the weaponisation of everything".

turns into sabotage – but evidence may still remain insufficient (at least to stand up in a court of law) and attribution prove elusive.

More fundamentally, these hostile "hybrid" activities are unconventional also in the sense that they cannot be countered in the same way conventional military (or even nuclear) ones can – that is, by matching and "parrying" an adversary's capabilities and actions. Externally, in fact, we do not necessarily want to "mirror" or replicate the methods of our attackers – be it disinformation, deception, corruption or coercion. No tit-for-tat, although some robust responses remain conceivable and executable. Internally, too, we do not want to restrict our own freedoms – of expression, organization, or ownership of business or media outlets – as our potential vulnerabilities also represent our declared strengths.

Finally, traditional conflict prevention and arms control mechanisms seem difficult to apply to the "cybrid" domain. First, the "weapons" are not (exclusively) state-owned, and states do not have the legal monopoly of the use of code (as opposed to the use of force). Second, by nature such "weapons" cannot be effectively monitored, inspected or disposed of, and they can easily be recreated anyway. Third, the current international climate seems hardly favourable to any fresh multilateral arrangement, especially in a domain where ongoing technological advances occur at lightning speed. Historically speaking, most arms control agreements were signed only after new technologies had matured and the resulting risks had been fully appreciated by the main stakeholders – and we appear to be still very far from that stage.

A long game

Despite all these constraints, however, there is ample room for strengthening our collective resilience (at both state and societal level) vis-à-vis the growing "hybridisation" of threats – wherever they may come from. Joined-up situational awareness is essential, and certainly requires better intelligence sharing than what we have now. Anticipation is also important, and technology may represent an asset and not just a liability in this area. Capacity and willingness to impose costs (both reputational and material) on attackers should also be part of the policy toolbox.[12]

Here NATO and the EU can provide a high degree of complementarity and potentially even synergy. Both can assist and advise their members in their areas of respective competence, e.g. through national points of contact, the activation of dedicated instruments and playbooks, the organization of crisis management exercises and the deployment of relevant experts – separately[13] and/or in parallel and coordinated fashion. Both can also resort to negative diplomacy and countermeasures to sanction hostile behaviour.

If "cybrid" is the new normal, and if the resulting campaigns cannot be completely deterred, then the name of the game is long-term sustainable containment

Still, responses need to be as targeted and tailored as the challenges are. Dealing with Russia and/or its proxies requires a different approach than dealing with Chinese operators or terrorist groups and their sponsors. Operating inside the Euro-Atlantic area will not be the same business as operating outside – in the East, in the South and notably in the South East, where different hybrid threats coexist and conflate. And cooperation is required not only between states and between international organizations but also between them and the private sector, which often owns and operates the "spaces" where those activities take place. If "cybrid" is the new normal, and if the resulting campaigns cannot be completely deterred, then the name of the game is long-term sustainable containment.

12 The spectrum of applicable policy responses is often referred to as DIMEFIL (Diplomatic, Information, Military, Economic, Financial, Intelligence, Legal) or just DIME.

13 For instance, NATO is about to deploy to Montenegro (at its request) a first dedicated Counter Hybrid Support Team. CHSTs were established in July 2018 and consist of national experts appointed by nations in fields as diverse as cyber defence, energy security, intelligence and counter-terrorism, civil preparedness, strategic communications, logistical and legal assistance.

Research Division
Thierry Tardy, PhD, Series Editor
NATO Defense College
Via Giorgio Pelosi 1, 00143 Rome – Italy
website: www.ndc.nato.int

Follow us on Twitter and Facebook
at *https://twitter.com/NDC_Research*
at *https://facebook.com/NDC_Research*
NDC Policy Brief
ISSN 2617-6009