BRIEF ISSUE 32 2015

Hybrid: what's in a name?

by Jan Joel Andersson and Thierry Tardy

Security analysts and practitioners have a tendency to coin new terms which capture the challenge(s) they are facing or the mandate(s) they are supposed to embrace. Terms such as 'low-intensity conflicts', 'failed' or 'fragile' states, 'asymmetrical' threats or even, for that matter, 'comprehensive approach' are all relevant examples. 'Hybrid threats' is, potentially, another case in point.

The concept of 'hybrid threats' is not new, nor is the idea that it conveys completely original – namely, the combination of conventional and unconventional methods of warfare so as to confuse an adversary. Russia's hostile actions in Ukraine and the violence perpetrated by the Islamic State of Iraq and the Levant (ISIL) in several areas neighbouring Europe – and within Europe itself – are oft-cited examples of these hybrid threats. It could, however, also be argued that Western countries have resorted to these methods themselves, albeit without calling them 'hybrid', and that warfare itself has never been 'pure'. But what is certain is that the European Union now considers itself a potential target of such threats and feels ill-prepared to respond.

The need for conceptual clarity

The May 2015 Foreign Affairs Council invited the HR/VP 'in close cooperation with Commission services, the European Defence Agency and in consultation with the EU member states, to present by the end of 2015 a joint framework with actionable proposals to help countering hybrid threats and foster the resilience of the EU and its member states as well as partners.'

As is often the case with such new concepts, there is a debate as to whether conceptual clarity is needed in order to craft a sound policy response or whether constructive ambiguity is preferable.

The first line of EU response to hybrid threats proposed by the EEAS involves 'improving awareness', and a key element of this is establishing a clear understanding of what exactly hybrid threats are, i.e. how they differ from 'non-hybrid' ones. Simply put, for a threat to be of a 'hybrid' nature it needs to be the product of multiple ways to threaten or attack its intended target – much as a hybrid species is produced by combining different breeds or varieties. It is therefore the *mix* of different methods – conventional and unconventional, military and non-military – which makes a threat hybrid.

In this sense, not all contemporary threats are hybrid. For example, a terrorist group which mainly plants bombs or makes use of suicide bombers does not, in and by itself, constitute a hybrid threat.

It is only if and when such an outfit combines such tactics with, for example, the launching of military campaigns, systematically spreading disinformation or running criminal activities that the threat mutates into a hybrid one. Terrorism, cybercrime, trafficking and extortion are not *per se* hybrid in nature; they may become so depending on how (and to what extent) they are pursued using multiple tactics simultaneously.

It may even be the case that some threats emanating from a particular organisation or state are hybrid while others coming from the same agent are not. The assessment of threats must therefore be constantly reviewed in light of new developments.

In general terms, hybrid threats are characterised by:

- the combination of conventional and unconventional, military and non-military, overt and covert actions;
- the aim of creating ambiguity and confusion on the nature, the origin and the objective of the threat;
- the ability to identify and exploit the vulnerabilities of the targets;
- the capacity to keep the level of hostility *below* the 'threshold' of conventional war.

Beyond the comprehensive approach

The multi-layered and multi-faceted nature of hybrid threats calls for an equally multi-pronged response, theoretically embracing the widest range of actions with a view to 'building resilience' and 'responding to attacks'. Here, the EU's 'comprehensive approach' comes to the fore, as it *a priori* provides an appropriate framework for policy response and an added value for the Union. The key challenge is to correctly calibrate the civilian-military balance of the response.

So far, the thinking on countering hybrid threats has largely been military-centric, in particular in the context of NATO. Yet the non-military and predominantly unconventional nature of hybrid threats arguably requires them to be tackled also – and possibly, in some cases, mainly – through non-military means.

Most importantly, in an EU context, it is the mix of *external* and *internal* security policies and instruments which is likely to provide the most appropriate response. Consequently, the comprehensive approach, insofar as it is mainly about the EU's external action, would need to be broadened so as to include elements of internal security.

'Hybrid threats' as seen by others

The term 'hybrid warfare' first appeared in 2002 in a thesis written by William J. Nemeth at the US Naval Postgraduate School ('Future War and Chechnya: a Case for Hybrid Warfare').

In the **US**, the term 'hybrid' does not appear in any of the last three National Security Strategies (2006, 2010, 2015). The 2015 National Military Strategy talks about 'hybrid conflicts' that may consist of 'military forces assuming a non-state identity, as Russia did in the Crimea, or involve a violent extremist organisation (VEO) fielding rudimentary combined arms capabilities, as ISIL has demonstrated in Iraq and Syria. Hybrid conflicts also may be comprised of state and non-state actors working together toward shared objectives, employing a wide range of weapons such as we have witnessed in eastern Ukraine. Hybrid conflicts serve to increase ambiguity, complicate decision-making, and slow the coordination of effective responses.'

The **UN** talks about 'asymmetric threats' (in peace operations) but does not use the term 'hybrid'.

The latest **NATO** Strategic Concept (2010) also does not mention the term 'hybrid'. However, the document titled 'NATO 2020', prepared by a group of 'wise persons' for the 2010 Lisbon Summit of the alliance, did note the 'hybrid variations' of threats. The 2014 Wales Summit Final Declaration refers to 'hybrid warfare threats' where 'a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design'. Furthermore, the 25 June 2015 Statement by NATO Defence Ministers talks about 'hybrid threats', for which 'we will seek close coordination and coherence with the EU's efforts in this field.'

In operational terms, this means that any common EU-wide response to hybrid threats would need to feature a clear division of responsibilities and identify synergies between three sets of actors/instruments: 1) *member states'* instruments and activities; 2) EU *internal* security instruments, i.e. freedom, security and justice tools, but also – and most importantly – those of the European Commission; 3) EU *external* security instruments (including CSDP operations and missions), and NATO activities.

One example which requires such an approach is the handling of 'foreign fighters', i.e. individuals who spend time in war-torn or lawless areas before returning and becoming potential threats to their own country (or others).

For any EU member state dealing with this issue, the response will combine exclusively national policies, cooperation at EU level on law enforcement, border controls and intelligence sharing, as well as possible EU initiatives aimed at capacity-building in third countries or disrupting hostile activities wherever they take place. This makes the coordination of various lines of response all the more vital, and takes them far beyond the current 'comprehensive approach' and any primarily military-focused response.

'In order to respond effectively, the EU not only has to develop a cyber-security strategy, a maritime strategy or a broader 'global' strategy; it must also learn how to synchronise all these aspects – and in a tailor-made fashion.'

In the meantime, the confusion intentionally created by hybrid tactics is likely to further complicate the ability of EU countries and institutions to craft a truly coherent and comprehensive response. In order to respond effectively, the EU not only has to develop a cyber-security strategy, a maritime strategy or a broader 'global' strategy; it must also learn how to synchronise all these aspects – and in a tailor-made fashion.

That said, the first and arguably main line of response will likely lie with the *member states*. The EU, therefore, needs to demonstrate its added value when it comes to improving awareness, building resilience, and responding to attacks. In this effort, the Commission is likely to be better equipped than CSDP.

E pluribus una

In any case, both the EU (through its various institutions, bodies, DGs and agencies) and its member states will have to develop generic responses to what are, in reality, very different types of threats. The Ukraine crisis and the emergence of ISIL occurred concomitantly in the spring of 2014, thus allowing for a conceptual but somewhat artificial grouping of the two threats under a common 'hybrid' label. In practice, however, policy responses are likely to be distinct and, possibly, differ significantly from one case to the other.

Indeed, this has been the case to date at all the three of the aforementioned levels (awareness, resilience, response). Can a generic policy response be designed to usefully address threats that, by nature, vary greatly in their 'hybridity'? Ultimately, the very heterogeneity of hybrid threats may cast doubts on the utility of developing a general, catch-all strategy to counter them.

As stated above, hybrid threats are generally considered to be hostile campaigns below the level of recognised war which combine conventional and unconventional, military and non-military, overt and covert actions aimed at creating confusion and ambiguity on their nature, origin and objective. Since these actions do not take place in wartime (legally speaking), the primary responsibility for directing any response is, in most countries, *civilian*. Similarly to traditional terrorist threats or attacks, it is the national police and civilian judicial authorities that are in charge of prevention and response.

The military dimension

However, the non-military component of hybrid threats should not hide the fact that the conflict(s) in Ukraine and the success of ISIL in the Middle East region have brought territorial defence and homeland security back onto the agenda in Europe.

While an outright military attack on any EU or NATO member state remains unlikely, the dangers of hybrid operations against the Union and its partners are real. After some 20 years of focusing on overseas international crisis management operations, the EU and its member states are now facing the challenge of building appropriate capabilities to address such new contingencies and threats.

Among these are also military capabilities proper. It is imperative that a military should have the capability to:

- *act as a deterrent*. No EU member state is strong enough to withstand a large-scale Russian operation on its own, but even a smaller yet capable military force will impact the calculation for any opponent contemplating hybrid operations;

- *quickly react even without outside help*. If a group of 'little green men' lacking visible insignias were

to occupy a village in an EU or NATO member state bordering Russia, that country's military and security forces must have the capability to rapidly respond on their own. The very nature of hybrid operations makes rapid collective defence responses difficult – if not near impossible – in consensus- and rules-based organisations such as the EU and NATO;

- *rapidly deploy to another EU or NATO member state in case of request and need*. While the US keeps a rotating force of 150 troops in each of the Baltic states and Poland since April 2014 (occasionally joined by similar-sized units from other NATO allies), more troops would be needed in the event of a crisis;

- *effectively support civilian authorities and police*. In cases of large-scale violent riots or acts of domestic terrorism associated with hybrid operations, police forces may be overwhelmed, contributing to the sense of confusion and hopelessness. In some countries, the police have the possibility to draw on military assets and personnel to act under civilian command. This capability could be further improved.

In all these cases, operational readiness will be important. In particular, special forces could play important roles in quickly establishing a military presence on the ground and providing intelligence in contested territories. Other important military assets in countering hybrid operations are airborne surveillance and remote sensor capabilities to provide necessary early warning and intelligence.

Strategic communications and defensive and offensive psychological operations ('psy-ops') are also central assets. Once a hybrid operation is successfully defeated, military capabilities may also be important for post-conflict peace-stabilisation missions. Such missions could include tasks like policing semi-permissive environments and would require close cooperation with civilian actors.

Old challenges, new strategies

By definition and nature, hybrid threats challenge the traditional boundaries (bureaucratic, legal, and operational) between military and civilian, public and private, national and collective capabilities.

Cyberattacks and online activities are typical cases in point: they are both enablers of action and actions in their own right; they call into question existing silos and competencies; they have – but also represent – moving targets; and they are often outsourced and not easily attributable.

This is where 'intelligence' in a broad sense (including monitoring, surveillance, early warning and preparedness) comes to the fore as a crucial capability to share and consolidate across geographical borders and functional boundaries. This is so at all stages and levels: awareness, resilience, and response proper.

It should also be remembered that today's focus on hybrid threats demonstrates a certain lack of institutional memory. While not called 'hybrid' during the Cold War, many analysts believed that covert or subversive acts would precede any Soviet attempts of regime change in neighbouring or neutral states in Western Europe. The fear that Soviet propaganda and disinformation could influence and intimidate domestic audiences and governing political structures was very real. Of course, some Western countries also engaged in their own overt and covert information campaigns against the Soviet Union and its Warsaw Pact satellites.

Clearly, much has changed since the days of the Cold War: digitalisation, the internet revolution, and the emergence of social media have completely transformed the landscape. Equally important, domestic populations in Europe are today more culturally and ethnically diversified than ever.

Last but not least, publics have less faith in authorities and senior public figures. Nevertheless, both defensive and offensive tactics and strategies used in the past still provide some useful insights when attempting to understand and counter the current hybrid challenges.

Jan Joel Andersson and Thierry Tardy are Senior Analysts at the EUISS.

This text was originally part of a research paper prepared by the EUISS for the European Defence Agency (EDA).

 | QN-AK-15-032-2A-N | ISBN 978-92-9198-288-2 | ISSN 2315-1110 | DOI 10.2815/422877