United in Ambiguity?
EU and NATO Approaches to Hybrid Warfare and Hybrid Threats

Jan Jakub Uziębło
United in Ambiguity?
EU and NATO Approaches to Hybrid Warfare and Hybrid Threats

Jan Jakub Uziębło
About the Author

Jan Jakub Uziębło is a College of Europe alumnus with an MA in EU International Relations and Diplomacy Studies. He also holds an MA in European Affairs from Sciences Po Paris and a BA in Politics with International Relations from the University of York. During his studies, he specialised in international and European security, EU-NATO cooperation and hybrid threats. The author currently works at the NATO International Military Staff, focusing on cooperation with international organisations. The opinions given in this paper are those of the author only. This paper is based on his Master’s thesis at the College of Europe (Chopin promotion), made possible by a scholarship from the Ministry of Foreign Affairs of the Republic of Poland.
Abstract

‘Hybrid warfare’, sometimes known as ‘hybrid threats’, became a trendy buzzword in recent years, used to describe a panoply of seemingly different threats. While neither the European Union (EU) nor the North Atlantic Treaty Organisation (NATO) appear to have a clear definition of this term, both organisations are taking steps to ‘counter hybrid’. This paper explores why this terminology has been adopted by both organisations and seeks to understand how this semantic choice influenced their respective policy responses as well as their cooperation. By analysing what hybrid means and which actors are designated with this label, I show that both NATO and the EU used hybrid to describe their vulnerability to a rapidly changing strategic environment. Although no final definition of hybrid has materialised, the term has allowed for increased informal and formal NATO-EU cooperation.
Introducing ‘hybrid’

“No-one should be under any illusion but that the threat posed by hybrid warfare is real”, read the website of the European People’s Party Group in April 2016. Such ominous statements became a constant feature of the political, media and academic landscape in recent years. In Europe and across the Atlantic, think tanks organised events on hybrid, publications multiplied and policy-makers at times managed to grasp a headline with a catchy reference to hybrid threats or war. Hybrid is a buzzword, and as such it is remarkable for its evolution as well as for the fact that no agreed definition for it has so far emerged. While the term has been used across the Atlantic for over a decade, it has only slowly gained popularity in Europe. Given the importance hybrid gained for both the North Atlantic Treaty Organisation (NATO) and the European Union (EU), it seems crucial to analyse how we arrived at a point where both organisations issued strategies seeking to ‘counter hybrid’.

To explain these developments, this paper seeks to comparatively assesses EU and NATO approaches to hybrid by seeking to answer two questions: Why has hybrid been adopted as the terminology of choice by both NATO and the EU to describe their security environment? To what extent has this semantic choice influenced actual policy responses and the cooperation between the two organisations?

The hypothesis guiding my analysis is that both organisations adopted hybrid because of their perceived vulnerability to a changed security environment. More importantly, hybrid seems to have become a catalyst for increased EU-NATO cooperation, notably carrying an important symbolic dimension. To verify this hypothesis, it is first imperative to understand how hybrid evolved as a term. Second, a precondition for understanding concrete EU or NATO policies is to identify threats which were designated as hybrid. Lastly, after analysing the respective NATO and EU responses to hybrid, EU-NATO cooperation on the subject needs to be analysed.

Given the qualitative nature of this analysis, as well as the sparse availability of unclassified sources, my work combines the analysis of primary sources and secondary literature, enriched by interviews conducted with NATO and EU officials and academics. This allowed me to gain insight into the real perception of hybrid within the two institutions, meaning, however, that my analysis is the sum of a range of subjective perceptions of the term and accompanying institutional processes.

1 European Parliament, EPP Group, The supreme art of war is to subdue the enemy without fighting, Brussels, 19 April 2016.
Getting across the semantic minefield

Hybridity became very fashionable in academic and policy-making circles in recent years. As with any neologism, the precise meaning of the term is still very fluid and adaptable to the situation which is being described. The semantic dust has therefore not yet settled on an agreed definition, meaning policy-makers use the term to describe emerging challenges, while academia is racing to coin a workable definition or model for hybridity. This section aims to show how hybrid came to be, which elements were perceived as constitutive of hybridity and which challenges the use of this terminology inevitably triggered.

The first time hybrid was used to describe war, has been dated to a thesis written in 2002 by W. Nemeth. Since then, the term gradually gained popularity within military circles, especially in the US Marine Corps, and was subsequently adopted by the US Department of Defense in order to capture the evolving character of conflict. One military theorist, LtCol. Frank Hoffman, significantly contributed to the popularisation of the term, studying hybrid war through historical examples of deliberate creation of uncertainty within the battlespace. As Freedman noted, hybrid warfare gained popularity after being used by Hoffman to describe Hizbullah tactics simultaneously employing conventional and guerrilla modus operandi in the 2006 Lebanon war. The term only proliferated from 2008 onwards, however, largely due to NATO and its Allied Command Transformation. The interconnected nature of military and policy circles within NATO was indeed the vehicle through which hybrid warfare was mainstreamed. Throughout its journey, this neologism kept evolving, with each use picking up more constituent elements, so that it “was no longer limited to a specific portion of the capability spectrum between irregular and conventional warfare, but now started to embrace any aspect related to the increasing complexity of modern conflicts”. Crossing the Atlantic naturally made the term more vulnerable to the use by a broader range of actors with different threat prioritisations, all perceiving novel elements in their individual security environments. Thus, some argue that “[e]ach member state, sub-agency or center of excellence understood [hybrid warfare] its own way, so that they could use it to push their

---
4 Ibid.
7 Ibid.
own agenda”. In sum, hybrid became a tool for describing situations which did not fit existing definitions of warfare, and it was already in use at NATO when the illegal annexation of Crimea and destabilisation of the East of Ukraine by Russia took place. Hybrid war was thus adopted for describing these unexpected Russian actions, which did not fit within existing NATO concepts.

The interlinked nature of the security and defence policy circles in Europe ensured the amalgamation of many additional elements within the main hybrid warfare/threats terminology. While hybrid was gaining popularity, other terms such as ‘ambiguous warfare’ (reportedly preferred by the United Kingdom), ‘limited’, ‘nonlinear’ or ‘special’ war, were losing ground. Not surprisingly, terms like the Cold War-era ‘political warfare’ made a return in the literature, and hybrid warfare was regularly compared to ‘asymmetric’ or ‘irregular’ warfare, two terms described by some as lacking “any discernible analytical value”. One interesting term, ‘the grey zone’, made its appearance more recently, and is paradoxically broader than hybrid warfare itself. As Paul aptly noted, “[i]ke hybrid threats, if everything is in the grey zone, then nothing is”.

A good starting point to provide an overview of elements which make hybrid warfare or threats hybrid in expert literature, seems to be Hoffman’s definition, as he largely contributed to establishing hybrid in US military thinking:

Hybrid wars can be conducted by both states and a variety of non-state actors. [They] incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. These multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects.

---

8 Ibid.
10 Freedman, op. cit., RUSI, p. 6.
12 Giles, op. cit., RUSI, p. 6.
14 F. Alamir, “‘Hybrid Warfare’: A Possible Trigger for Advances in the Comprehensive Approach?”, Ethics and Armed Forces, no. 2, 2015, p. 3.
16 Hoffman as cited in M. Miller, Hybrid Warfare: Preparing for Future Conflict, Air War College, Air University, Maxwell AFB, AL, 2015, p. 7.
His take on hybrid warfare is confined to the battlespace, seeking to denote a departure from conventional warfare through increased complexity. Another definition, from a 2010 NATO Capstone project, defined hybrid threats as “those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives”, showcasing the view that a simple combination of different elements was making a threat hybrid. Subsequent definitions, however, included a broader range of understandings, the only common thread being a disclaimer stating that hybrid is in fact nothing new. If so, why use it?

I understand definitions of hybrid warfare and hybrid threats as putting the emphasis on three core elements: dynamism, complexity and simultaneity. As some authors note, “hybrid wars are complex, because they don’t conform to a one-size-fits-all pattern”. They involve a plurality of actors (both state and non-state) and present “tactics [which] can be scaled and tailor fit to the particular situation”. Suggesting a dual nature of its component parts, hybrid is inherently heterogeneous and, as Drent and others observe, the “core strength of hybrid warfare is that it can morph in nature [which] results in (the possibility of) constantly differing encountered and observed characteristics”. What seems crucial here, is the departure from clear-cut goals of military action. As Kramer and colleagues point out, “[p]ractitioners of hybrid warfare are often less intent on seizing and holding territory than destroying or disrupting the ability of societies to function”. Other researchers illustrated the difficulty of defining hybrid by pointing out that one agent can present both a hybrid and a non-hybrid threat, thus necessitating “conceptual coherence”.

In this respect, it is worth noting that there is no clear differentiation between definitions of hybrid threats/warfare. As illustrated by the US Government Accountability Office, similar

20 J. Miranda-Calha, Hybrid Warfare: NATO’s New Strategic Challenge?, NATO Parliamentary Assembly, 166 DSC 15 E bis, 2015, p. 3.
21 Jacobs & Lasconjarias, op. cit., p. 2.
24 EUISS, op. cit.
definitions were applied to both terms within the same departments. 25 In Europe, understandings of hybrid warfare or threats also vary significantly from one official to another.

By virtue of its popularity, hybrid warfare lent itself to significant criticism since its emergence. Besides the inherent imprecision26 of this terminology, many authors took issue with the use of the word ‘war’ to describe activities in the diplomatic, information, economic or energy domains.27 One of the fiercest critics of the term has been Elie Tenenbaum. Comparing the concept to an “auberge espagnole stratégique”,28 the author denounced the fact that it “has been diluted to the point of absurdity”.29 Tenenbaum saw the use of force as the necessary element for the application of this label30 and the hybrid warfare terminology as critical for the bureaucratic survival of many NATO support structures such as think tanks and centres of excellence (COEs) which, for him, deliberately skewed the meaning of the concept to fit their competence area.31

Other critics are even more sceptical. While some see hybrid warfare as “nothing more than a semantic brand for the current practice of ‘muddling through’ in security policy”,32 others interpret it as “[t]he West [...] terrorizing itself with specters of hybrid war to an extent that it should qualify as one of history’s better disinformation operations, even if it was wholly unintentional”.33 “Frustration” with the term, has even led experts like Sven Biscop to write pieces against its use,34 arguing that “one cannot make strategy against an adjective”.35 As for solutions, Van Puyvelde advocated in a similar vein that “decision-makers should stay away from [hybrid] and consider warfare for what it has always been: a complex set of interconnected threats and forceful means waged to further political motives”.36 Returning to past ways of conceiving warfare, however, carries the risk of ignoring the fundamental idea at the core of the hybrid concept, namely that something has changed.

28 Ibid., p. 9.
29 Tenenbaum, op. cit., NATO Defence College, p. 95.
30 Tenenbaum, op. cit., IFRI, p. 22.
31 Ibid., p. 35.
33 Kofman, op. cit.
34 Interview with Prof. Sven Biscop, Director Egmont Institute, Bruges, 9 March 2016.
Based on these considerations, I propose the following definition of the ‘hybrid opponent’: Seeking to exploit the full range of a target’s weaknesses, a hybrid opponent possesses the capacity of simultaneous escalation, at different points along the broadly-defined spectrum of conflict, transcending the battlefield at will to target state or society. Constantly adapting, a hybrid opponent can use different channels and proxies, often making attribution difficult, using unlawful actions and, at times, seemingly acting without a clear strategic objective.

To conclude this part, while some maintain that “hybridity indicates the indefinability of the thing so described”, others believe that it offers positive insights which justify continued refinement by academia. In this respect, Hoffman argued that,

> [i]f at the end of the day we drop the “hybrid” term and simply gain a better understanding of the large gray space between our idealized bins and pristine Western categorizations, we will have made progress.

Similarly, Reichborn-Kjennerud and Cullen argued that hybrid is a “useful concept”, seeing it as highlighting the “intellectual challenges adversaries are bringing to the table in terms of what war is and how it should be understood”. This warrants an analysis of which threats are labelled as hybrid.

**Hybrid in a changing strategic landscape**

The hybrid warfare/threat terminology was inevitably shaped by the timeline in which it emerged. Reichborn-Kjennerud and Cullen argue that hybrid warfare “was deduced from looking at the enemy, thus shifting its definition and meaning, according to the subject of analysis”. Understanding to whom this label is ascribed is thus a precondition for understanding any policy responses to hybrid.

Hybrid warriors – they came from the East

In Western perceptions, Russia is the embodiment of an actor conducting hybrid warfare. As Johnson notes, after the start of the Russian aggression on Ukraine, its actions were “initially
labelled by some in the West [...] as ‘hybrid’ warfare and treated as a new phenomenon”.43 This speaks to the element of ‘surprise’, making hybrid warfare a quick fix for an inability to explain events, which only a handful of experts have anticipated. The fact that hybrid became the prevalent terminology to describe Russia’s actions does not necessarily help our analysis, as “what Russian hybrid warfare is and how it works, varies dramatically depending on what report or PowerPoint brief you are reading”.44 Although an extensive analysis of the Russian hybrid threat is outside the scope of this work, some elements are needed.

According to Maj. Davis Jr., “[t]he Russians have been able to combine various military forms of warfare with economic, information, and diplomatic [instruments of power] into essentially a hybrid threat whole of government approach”.45 As elaborated by Ruiz-Palmer, “hybrid warfare bridges the divide between the hard and the soft power applications that result from the technological and information revolutions of the last three decades in ways that maximize asymmetric advantages for Russia, as well as minimize risks and costs”.46 This hints at a perception of Russia having a clear strategic design and a hybrid methodology to carry it out cost-effectively. This approach is illustrated by some publications stating that “[a] clear goal of Russia’s use of hybrid tactics is to sow doubts about the nature and severity of the threat any particular action may pose”.47 On the other hand, experts argue that “against the backdrop of Russian aggression against Ukraine [...] even routine military behaviour translates into a signal”, 48 pointing to the importance of perception and own vulnerability.

The above-mentioned examples serve to illustrate my point that, not only was hybrid warfare, as Reichborn-Kjennerud and Cullen argued, “deduced from looking at the enemy”,49 but it was also deduced by looking in the mirror – the product of a sudden realisation of Western weakness and vulnerabilities when faced with an increasingly uncertain environment. In this respect, Ruiz Palmer argues that,  

Russia’s adoption of hybrid warfare is the product of a combination of strategic opportunity and necessity, tailored to today’s environment of heightened societal connectivity, fragility and vulnerability – the opportunity to pursue and achieve policy

44 Kofman, op. cit.
45 Davis, op. cit., p. 23.
47 Miranda-Calha, op. cit., p. 4.
objectives of the highest importance through the active, but calibrated, employment of mostly non-military means, together with the necessity to avoid a highly destructive, and potentially decisive, use of force by an adversary.\textsuperscript{50}

This idea helps explain the initial opposition of Poland, the Baltic states and others to the “framing of Russian operations within a concept of hybridity”,\textsuperscript{51} since they saw it as avoidance of concrete actions to counter Russia in the event of an operation “categorized as being under a threshold of war”.\textsuperscript{52} Early reluctance of these states to classify Russian actions as hybrid was thus paradoxically an expression of vulnerability to what is routinely accepted to be part of hybrid warfare: the sewing of divisions within intergovernmental decision-making systems.

The hybrid debate led authors like Thornton to conclude that “[t]he West must adjust to the situation in which it now finds itself in relation to Russia – a ‘permanent’ hybrid war”,\textsuperscript{53} referring to Russian General Gerasimov.\textsuperscript{54} Although understanding Russia through this ‘Gerasimov doctrine’ became popular in some circles, it has largely been dismissed as a case of “buzzwords becoming fixed features of our cognitive landscape, simply because they fit neatly on a PowerPoint slide”.\textsuperscript{55} To be precise, making sure to base one’s analysis on facts does not diminish Russia’s revisionist and illegal actions. The principal question, however, is to distinguish between truly novel elements and ones in which the sole innovation is the “exploitation of ambiguity, both of intent and attribution”, which itself is drawing on previous Russian and Soviet practices.\textsuperscript{56}

Being able to evaluate intent seems paramount. Indeed, while some see Russian actions, for example in the information sphere, as “opportunistically [trying] to ‘stir the pot’ of public discontent and distrust”, the difficulty lies in determining whether this is an integral part of a fully articulated strategy.\textsuperscript{57} Providing an answer to this question lies beyond the scope of this work, but does point to the underlying problem of “the loss of analytical depth and institutional memory […] to examine Russia’s intentions and aspirations”,\textsuperscript{58} as has been further demonstrated by ongoing discussions of Russian ‘meddling’ in various Western elections.

\textsuperscript{50} Ruiz-Palmer, op. cit., p. 50.
\textsuperscript{51} Giles, op. cit., RUSI, p. 7.
\textsuperscript{52} N. Schadlow, “The Problem with Hybrid Warfare”, War on the Rocks, Online Article, April 2015.
\textsuperscript{54} Ibid., p. 42.
\textsuperscript{55} Giles, op. cit., RUSI, p. 10.
\textsuperscript{56} Johnson, op. cit., p. 137.
\textsuperscript{57} Kofman & Rojansky, op. cit., p. 6.
\textsuperscript{58} Giles, op. cit., RUSI, p. 61.
Parallel Southern Threats

The hybrid threat known as the Islamic State will inevitably thrive if we collectively fail to [...] encourage new models of government that guarantee basic human rights while respecting prevailing cultural norms.59

Evidence of a parallel diffusion of hybrid terminology within separate expert circles is illustrative of the dilemmas institutions like NATO or the EU face today. Indeed, problems with delimiting the scope of what constitutes hybrid were particularly well captured by US Secretary of Defence Ash Carter arguing that

[hybrid warfare] has two aspects to it [...]. One is terrorism, which is sub-state actors wielding that destructive power. Unfortunately there are also states that use the same instruments and the same vulnerabilities for more traditional purposes. And that’s true whether it’s little green men in Ukraine. Or, as to be blunt about it and something we’ve objected to, actors in China stealing intellectual property and not being apprehended and stopped from doing it. [From] China to the Iranian government aiding the Houthis or contributing to Hezbollah. This kind of thing also, that’s what hybrid warfare is.60

With similar semantic generosity, a European Parliamentary Research Service document provides an extensive list of hybrid threats, which include among others, Russian special operations in Ukraine, terrorist organisations, state-affiliated hackers, drug cartels, China’s policies in the South China Sea, as well as resource scarcity.61

While France used hybrid “in its 2013 defense review with the jihadist nexus in Sahel in mind”, in the current European strategic environment the other major hybrid threat besides Russia, is perceived to be the Islamic State (IS).62 As described by the NATO Parliamentary Assembly, “[IS] can be termed a hybrid threat due to its effective ability to employ a range of tactics from terrorist to conventional and its global recruitment networks to rally thousands of fighters to its cause”.63 This speaks to the idea that hybrid became a shorthand used to describe actors threatening Western vulnerabilities, or even to denote the use of instruments of statehood one disagrees with. A paradoxical dimension of this has been captured by Drent and others, who noted that both the IS’s modus operandi of publicising its acts of

---

62 Tenenbaum, op. cit., NATO Defence College, pp. 97-98.
63 Miranda-Calha, op. cit., p. 7.
violence to generate fear and recruitment, and Russia’s denial of involvement in the Donbass, were perceived as hybrid.64

Finally, a refreshing approach for understanding which threats deserve this label might be to proceed by elimination. As Gunneriusson and Ottis very aptly put it,

Hybrid threats are not defined by the actors, since states, non-state actors and even individuals might be considered (part of) hybrid threats. They are not about some specific technology, since the list here keeps growing as new technologies become available. They are not about specific effects, as a hybrid campaign may result in casualties, changed decisions, altered public perception, etc. Perhaps the best way to put it, hybrid threat is a manifestation of total war.65

In sum, I see hybrid terminology as conducive to apophenia (meaning the tendency of seeking patterns) and leading to an amalgamation of diverse threats, at the risk of disregarding key differences between them. Having shown a parallel diffusion of hybrid terminology to denote a wide range of threats, the next step is to evaluate whether this semantic ambiguity translated into policy responses meant to ‘counter hybrid’.

A changing understanding of war

Hoffman argued that our Russian and Chinese competitors “do not delude themselves with neat orthodoxies about categories and Clausewitizian models about how ‘real wars’ are fought and won” and that “[n]either should we”.66 This idea is based in part on the work “Unrestricted War”, written in 1999 by two Chinese People’s Liberation Army officers,67 in which they brought forth a broad conception of war reportedly including “all means, military and non-military, lethal and non-lethal to compel the enemy to accept one’s interests”,68 which “would require a shift in the minds and thoughts of the Western way of war”.69 It seems that with the advent of hybrid, a similar strand of thinking began materialising among Western policy-makers. Indeed, one does not have to look far to find examples of prominent figures stating that there is a “blur[ed] line between war and peace”, meaning that there exists “a state which is somewhere in between”.70 This idea is key to understanding the

---

64 Drent et al., op. cit., p. 23.
67 Ibid.
68 As quoted in USJFCOM, Irregular Adversaries and Hybrid Threats, Joint Irregular Warfare Center, 2011, p. 24.
69 Davis, op. cit., p. 21.
70 J. Stoltenberg, as quoted in US Department of Defense, op. cit.
debate about hybrid within both the EU and NATO, as it challenges the core of the Western institutional, legal and societal schemata for conceiving war.

This challenge for some is a need for conceiving war as “a joint civil/military venture, top to bottom”. Indeed, as Reichborn-Kjennerud and Cullen critically point out, conflicts no longer follow neat phases, fitting a model which can be used to elaborate appropriate responses, which can lead to interpreting hybrid war as a permanent state of war. As one official pointed out, “if you combine the dots, you get a picture that we are already under attack, under permanent attack”. In this context, situational awareness is key, but it is the very nature of our systems of governance which can be seen as impeding an effective adaptation to hybrid. Indeed, if hybrid war is perceived as being waged “with at least a certain degree of central control”, the very identity and institutional set-up of Western democracies not only restricts the capacity to carry out hybrid warfare, but places the West at a significant disadvantage compared to authoritarian systems. Indeed, nowadays the key concern remains how to couple high military readiness with “the exercise of political agility in response to hybrid threat”, while vulnerability to salami tactics or “death by a thousand cuts” are often mentioned, especially at the intergovernmental level, which I will now evaluate starting with NATO.

Adapting NATO to hybrid war

With hybrid warfare becoming the buzzword of choice for NATO, unsurprisingly there was no common understanding of the term within the Alliance. As evidenced above, hybrid was already used by NATO in 2010, at a time when hybrid threats were understood as “those posed by adversaries, with the ability to simultaneously employ conventional and non-

72 Reichborn-Kjennerud & Cullen, op. cit., p. 3.
75 A. Cederberg & P. Eronen, “How can Societies be Defended against Hybrid Threats?”, GCSP Strategic Security Analysis, Geneva Centre for Security Policy, no. 9, 2015, p. 4.
76 Alamir, op. cit., p. 4.
78 Paul, op. cit.
79 Jacobs & Lasconjarias, op. cit., p. 2.
conventional means adaptively in pursuit of their objectives". Already then, there was a growing realisation that NATO is ill-suited to face these threats, the response to which would “likely depend on factors outside the current remit of the NATO military sphere”. I will now analyse how hybrid warfare came to be interpreted within NATO and which policy responses were sought.

From different perceptions to a comprehensive approach

Despite authors like Lindley-French stating that, for NATO, hybrid warfare “exploits political [and societal] seams” (using pressure, propaganda, proxies and psychological operations), differentiated perceptions of hybrid were quick to surface among NATO officials. For example, within the team tasked with developing the Alliance’s approach towards hybrid warfare, one official working on the issue confirmed that he did not particularly like how hybrid became an established term, as for him “it is just warfare in the 21st century, where an opponent can use every lever in his power”. His team thus had to work with a term which “everybody agreed was not overly useful”, trying “not to put it on a pedestal”, but instead focusing on Russian actions in Ukraine. This also seemed to be the dominant view among NATO Allies, which reportedly tried “to avoid using the term as much as possible”, instead organising separate discussions on different threats simply because “everybody understands hybrid differently”. One senior official confirmed this by saying that, for him, hybrid warfare was “useful from a bureaucratic point of view, raising the issue up the agenda” and allowing “to get the military involved in defence planning and developing crisis response measures” – in short, guaranteeing a sustained level of attention. The official acknowledged however that this “is not just a bureaucratic exercise”, because NATO actually “sees hybrid as a form of warfare”, aiming to destabilise and render a country more “attackable”.

Hybrid was described by some as bringing “a useful, holistic understanding of the security challenges from both the East and the South”, which “provides tools for a

---

82 Lindley-French, op. cit., p. 1.
83 Interview with A. Budd, Head of Defence Capabilities Section, Defence Policy Planning Division, NATO, via telephone, 4 April 2016.
84 Ibid.
85 Interview with anonymous NATO member state diplomat, Brussels, April 2016.
86 Interview with Dr. J. Shea, Deputy Assistant Secretary General for Emerging Security Challenges, NATO, via telephone, 31 March 2016.
87 Ibid.
comparative strategic perspective [...], while allowing for a differentiated response” to each.88 Indeed, this seems the approach which was adopted by NATO, pointing to an effort to ensure the buy-in of all Allies, despite their varying threat prioritisations. In the context of the run-up to the 2016 Warsaw Summit, NATO was focused on its Eastern flank, thus making officials ask “how can we stay ahead of Russia?” and describe hybrid warfare as a “game of whack-a-mole”.89 In addition, the possibility of simultaneous escalation along a broadly-defined spectrum of conflict is straining Allied structures. As remarked in a NATO White Paper, “[a]dversaries may trigger simultaneous and diverse crises using a hybrid form of warfare that challenges our planning, preparation and decision making processes”,90 thus carrying a significant risk given the principle of consensus within the organisation.91

Despite the hype around hybrid, NATO’s approach to hybrid warfare seems largely anchored in its previous buzzword: the comprehensive approach (a by-product of NATO experiences in Afghanistan and in the Balkans).92 Indeed, Secretary General Stoltenberg stated that “hybrid is the dark reflection of our comprehensive approach”,93 pointing to a certain continuity in NATO’s adaptation efforts.

Hybrid became a key part of these efforts, however, with the 2015 Report of the NATO Secretary General talking about “preparing for, deterring and defending against” hybrid warfare.94 Since one of NATO’s core tasks is collective defence, the notion of deterrence has long been part of its modus operandi. With hybrid, this question seems more complicated, as “hybrid is less ‘deterable’”.95 Although NATO officials seem to agree that “it is not useful deterring hybrid as such”,96 the idea of “deterrence by denial” is established within the Alliance.97 This concept, attributed to Glen Snyder, is based on reducing the perceived benefit of an action by hardening defences and augmenting the cost of a potential attack, as opposed to “deterrence by punishment”.98 As argued by Rühle, in the context of hybrid...
and its ambiguity, the latter form of deterrence is unlikely to succeed, making “deterrence-by-resilience” the natural choice for hybrid warfare defence planning. 99 Kramer and colleagues, in turn, show that “the requirement for resilience arises because hybrid war, including the capacity for cyberattack, has changed the landscape of conflict”.100 As stated by one diplomat, “resilience is the other term which had an incredible career recently”,101 and it is precisely the concept of resilience which was at the core of the 2016 NATO Warsaw Summit. 102 Indeed, “ensuring the survivability of government”,103 resilience of critical infrastructure, services104 and society, go hand in hand with NATO’s efforts to ensure the ability for quickly moving and deploying forces and equipment to Allied territory.105 Analysing Allied priorities in this context, it emerges that formulating concrete reassurance measures for the Eastern flank was prioritised over NATO’s work on a strategy to counter hybrid warfare (with some states deliberately delaying the latter).106

Ultimately, for NATO, since “[e]ach hybrid threat is different, and so is each of the 28 nations’ vulnerabilities”, it is only logical that “[n]ational governments are the first responders”,107 triggering the need to improve intelligence-sharing and establish “early warning indicators” of hybrid warfare.108 Indeed, for the Alliance “it appears that knowledge and anticipation are the best answer to hybrid threats”.109 This realisation is precisely what led NATO to develop guidelines to enhance national resilience to hybrid warfare110 as well as to establish a new civil-military Intelligence division, supplemented by sustained efforts to “persuade countries to share intelligence”.111

While Allies adopted assurance-focused measures through the Readiness Action Plan in 2014, and a strategy to counter hybrid warfare in December 2015,112 these developments should be seen as merely first steps in an overall NATO “strategic realignment”.113 Indeed, with NATO facing internal challenges and ones all along the Diplomatic, Information, Military,  

100 Kramer et al., op. cit., p. 1.  
101 Interview with anonymous NATO member state diplomat, op. cit.  
103 Interview with A. Budd, op. cit.  
104 Shea, op. cit., NATO Review.  
105 Ibid.  
106 Interview with anonymous NATO member state diplomat, op. cit.  
108 Shea, op. cit., NATO Review.  
110 Stoltenberg, op. cit., p. 18.  
111 Interview with J. Shea, op. cit.  
113 Lindley-French, op. cit., p. 7.
As a result, although member states are incentivised to engage in mapping their vulnerabilities to Russian influence in specific sectors such as energy, information, or finance, hybrid warfare mainly presents aspects which fall outside NATO's competence or capabilities.

One such area of pivotal importance is strategic communication where, to put it in Supreme Allied Commander Transformation’s words, “[NATO] has to gain the battle of the narrative”. In this respect, NATO Strategic Communications Centre of Excellence conducted a study on the use of social media “as a weapon of hybrid warfare”, focusing on the use of so-called ‘trolls’ by Russia. Moreover, addressing vulnerabilities within societies, which could “undermine trust in governments”, is key for the Alliance in establishing a “mind-set of defence […] in social and political venues”. NATO also seeks to foster resilience in the private sector, especially in cyber, where according to the Secretary General, “it’s actually possible to wage war in a time of peace”.

While before the Warsaw Summit Allies were seen as the first responders to hybrid, the Alliance has also taken concrete collective steps to address vulnerabilities, first focused on its Eastern flank, but increasingly also looking at how to project stability in the South. The overall adaptation can nonetheless be seen as following a linear path, largely anchored in the comprehensive approach and focused on deliverables it can showcase as examples of Allied solidarity. NATO’s approach to hybrid, in sum, can be described as pragmatic and the hybrid label as not particularly relevant. On the other hand, another actor seems to be particularly well fit for addressing hybrid, namely the EU.

---

114 Interview with A. Budd, op. cit.
117 Shea, op. cit., NATO Review.
118 NATO White Paper, op. cit., p. 10.
119 Ibid., p. 6.
120 NATO StratCom COE, Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia, Riga, 2016, p. 3.
121 Shea, op. cit., NATO Review.
123 J. Stoltenberg, as quoted in US Department of Defence, op. cit.
Europe countering hybrid threats

In general, the EU does not speak about hybrid warfare, preferring the phrase hybrid threats. There are nonetheless many exceptions to this rule. An anecdotal but telling example for the EU’s lack of coherence, was a video released by the Council of the EU, which provided the following definition of hybrid threats in its metadata: “[h]ybrid threats are a combination of military and non-military means. The objective is to destabilise opponents, create confusion, mask the real situation on the ground and hamper decision-making”.124 This speaks to the fact that, although the EU does not have an agreed definition of hybrid threats, an increasing number of policy responses were being drafted to ‘counter’ them, raising the need to develop ways to communicate on the issue to the public. In light of these responses, it is important to understand the EU’s approach to hybrid threats, which already in 2015 the EU’s High Representative Mogherini (HR/VP) called “the new normal”. 125

The beginning of an EU policy response to hybrid can be traced to the drafting of several member states’ non-papers on the issue in early 2015. One such non-paper, drafted by the Nordic Group,126 was presented at the informal meeting of EU defence chiefs in Riga in February 2015, focusing on Russia and calling for European unity.127 Similar documents were later drafted by France (focusing on the southern flank) and by Finland (focusing on resilience). Consequently, the Crisis Management Planning Directorate (CMPD) of the European External Action Service (EEAS) was tasked with developing an initial document for discussion, which was circulated in May 2015.128 Furthermore, both the Latvian and the subsequent Luxembourgish rotating EU Presidencies drafted unofficial background notes, providing context and recommendations on possible ways forward. Officially, however, the process started with the invitation by the May 2015 Foreign Affairs Council, to the European Commission and HR/VP to draft a joint framework on hybrid threats “with actionable proposals”, an invitation further reiterated by the June European Council.129

---

124 Council of the EU, Hybrid Threats, YouTube, 18 April 2016.
125 F. Mogherini, “Remarks by High Representative/Vice-President (HR/VP) Federica Mogherini”, EUISS Annual Conference, Brussels, 9 October 2015.
126 In this case 10/12 countries (Denmark, Estonia, Finland, Netherlands, Lithuania, Latvia, Germany, Norway, Poland and the UK).
127 Pawlak, op. cit.
128 Ibid.
The EU sought to take all member states’ concerns into consideration, through the organisation of consultations aimed at securing the buy-in for any EU-level solutions. Similarly to the misperception hybrid caused within NATO, this all-inclusive approach led to confusion within the EU. As a result, the European Commission pushed for creating a definition of the term, in order to clear the semantic and legal blurriness. Interestingly, the EU Military Staff initially drafted a document arguing against the use of hybrid terminology, which was ultimately discarded. This example of institutional disagreements over the utility of hybrid is indicative of a level of fragmentation and persisting ‘silos’ within EU institutions, even the ones located in a same building. Ultimately, a certain convergence finally emerged, characterised by one official as the need “to do something [...] at least speak the same language”. Similarly, another official asserted that hybrid is “just a bumper-sticker” and that in the end, it “does not need a definition [...] as long as we know what we mean by it”.

A difference to NATO is the EU’s consciously civilian approach. Drent and colleagues have shown that in the EU, in the context of hybrid, “the word ‘warfare’ is consciously avoided”, because of the opposition of certain member states. The EU’s ‘Joint Framework on Countering Hybrid Threats’ is illustrative of this. The document states that

> while definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods [...] which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.

I would argue that this rationalisation for a lack of definition seems to have been dictated by the inability to provide one, rather than a need for flexibility. This is illustrated by an earlier CMPD document on the subject stating that

> hybrid warfare can be more easily characterised than defined as a centrally designed and controlled use of various covert and overt tactics, enacted by military

---

130 Interview with Col. Calaresu, Military Assistant, CMPD, Brussels, 14 March 2016.
131 Interview with S. Bicop, op. cit.
132 Ibid.
133 Interview with Col. Calaresu, op. cit.
134 Ibid.
135 Interview with Mr. Gabor Iklody, Director of CMPD, EEAS, Brussels, 21 March 2016.
136 Drent et al., op. cit., p. 43.
137 European Commission & HR/VP, op. cit., p. 2.
and/or non-military means, ranging from intelligence and cyber operations through economic pressure to the use of conventional forces.138 These differences of perception are significant, especially given the initial prominence of the CMPD in shaping the EU’s overall response to hybrid, resulting in an approach similar to the one of NATO. Indeed, CMPD authors argued that “hybrid attacks” are “designed to exploit a country’s vulnerabilities”, can “generate ambiguity both in the affected population” and internationally with the “aim to swamp a government”.139 The emphasis on vulnerabilities, present in all member states, means mapping them – at times a sensitive issue – should be the first step towards building resilience.140 Nonetheless, if these vulnerabilities are present at the member state level, how does the EU see its role in countering them?

Many authors and officials asserted that the EU is “well placed” to counter hybrid threat.141 Despite this, the EU officially recognised that “responding to and countering [hybrid threat] is and will remain a national responsibility”.142 Indeed, the EU’s role is described as a “platform” for harmonising responses on specific issues like critical infrastructure,143 as well as providing an “added value” on awareness, resilience and response.144 This approach is thus one in which “a good number of the indicators and warnings from across the broad range of EU competencies” are already available,145 the challenge being “strengthen[ing] [the] ability to recognise, prevent, counter and defend against hybrid threats”.146 This can be seen in EU policy responses, as I will show below.

From ambiguous threats to catch-all policy responses

The EU’s approach to countering hybrid threat materialised in April 2016, when the Council welcomed “the Joint Communication on countering hybrid threat and fostering resilience of the EU and its Member States as well as partners”, and invited the Commission and the HR/VP “to provide a report by July 2017 to assess progress” on this topic. 147 The Council also

139 Ibid., p. 3.
140 Ibid., pp. 3-4.
141 Drent et al., op. cit., p. 43.
142 EEAS (CMPD), op. cit., p. 5.
143 Ibid.
144 EUISS, op. cit.
145 EEAS (CMPD), op. cit., p. 4.
146 Council of the EU, PMG Recommendations on Countering Hybrid Threats, 12265/15, 2015.
highlighted “the need for closer dialogue, coordination and cooperation with NATO”.\textsuperscript{148} These conclusions were a product of months of negotiations. Their actionable nature meant 22 actions were put forward in the ‘Joint Framework on Countering Hybrid Threats’.\textsuperscript{149}

While the tangible impact of this document should be the subject of a separate analysis, a brief examination is essential for understanding the EU’s responses to hybrid. First, it is crucial to note that actions relating to critical infrastructure form the bulk of EU responses, reflecting the Commission’s previous work in this area, but also the fact that critical infrastructure protection is relevant for both the southern and eastern dimensions of hybrid. As a result, the Commission is set to support energy diversification and resilience (including cyber), monitor emerging threats and develop responses concerning transport infrastructure (including cyber), increase the resilience of space infrastructure against hybrid threats, as well as improve awareness, cooperation and resilience in cybersecurity.\textsuperscript{150}

Another axis for proposed action are efforts to improve awareness and information-sharing, cutting through the ambiguity of hybrid (although the vagueness of these proposals is striking). Indeed, the HR/VP “will launch a hybrid risk survey” in the EU’s neighbourhood\textsuperscript{151} and support the member states in launching their own “hybrid risk survey”.\textsuperscript{152} Similarly, the Commission will aim to identify common tools and indicators for the protection of critical infrastructure, as well as “promote and facilitate information-sharing platforms and networks” in cyber-security.\textsuperscript{153} The flagship initiative to address the ambiguity of hybrid is the creation of “an EU Hybrid Fusion Cell” within the EU Intelligence and Situation Centre.\textsuperscript{154} This (very) small structure was designed to “see the patterns” of a ‘hybrid campaign’ in information provided by member states and EU bodies,\textsuperscript{155} while cooperating with NATO\textsuperscript{156} in order to provide top EU decision-makers with better situational awareness.\textsuperscript{157} Although limited in scope and needing time for implementation, this policy response has the merit of being new, as opposed to most actions which were in the legislative pipeline regardless of hybrid. One

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{148} Ibid.
\item \textsuperscript{149} European Commission & HR/VP, op. cit.
\item \textsuperscript{150} Ibid., pp. 7-12.
\item \textsuperscript{151} Ibid., p. 15.
\item \textsuperscript{152} Ibid., p. 3.
\item \textsuperscript{153} Ibid., pp. 6, 12.
\item \textsuperscript{154} Ibid., p. 4.
\item \textsuperscript{155} Interview with G. Iklody, op. cit.
\item \textsuperscript{156} EEAS (CMPD), op. cit., pp. 4-5.
\item \textsuperscript{157} EPSC, “From Mutual Assistance to Collective Security”, EPSC Strategic Notes, no. 10, 2015, p. 12.
\end{enumerate}
\end{footnotesize}
example is the ‘actionable proposal’ in the section dealing with “targeting hybrid threat financing”, which is a re-framing of an existing EU measure for fighting terrorist financing.158

It is worth exploring the idea of deterrence in the EU’s response to hybrid threats. Although one official asserted that in the EU “we do not deter”, the focus being on resilience,159 this seems inaccurate. Indeed, while the Joint Framework does not mention deterrence per se, several elements do point in that direction. Deterrence-like signalling within the text can be seen in the discussion of a possible invocation of Article 42 (7) TEU to provide a response in case of “multiple serious hybrid threats constitut[ing] armed aggression against an EU Member State”, as well as in the mention of a possible increased cooperation with NATO following “a wide-ranging and serious manifestation of hybrid threats”.160 Interestingly enough, in an area often cited as a potential EU strength on hybrid, namely the Union’s ability to impose sanctions, only the following sentence can be found: “[i]n the context of CFSP [Common Foreign and Security Policy] instruments, tailored and effective restrictive measures could be explored to counter hybrid threats”.161 Overall, although the EU indeed does not subscribe to the deterrence concept, this does not mean that it does not signal its deterrence-by-denial toolbox.162

To conclude, the EU’s response to hybrid threats can be seen as a mix of existing measures alongside new attempts to address vulnerabilities and improve situational awareness. To paraphrase one of the officials I spoke with, the EU’s approach is mainly reactive because only a specific combination of hybrid elements in a systematic fashion makes a campaign hybrid – adapting is therefore a question of mind-set.163 One of the aspects of this new mind set is to look for synergies with likeminded partners, as exemplified by NATO-EU cooperation.

**A hybrid partnership**

While NATO-EU cooperation outside of the ‘Berlin Plus’ arrangements is mired by political obstacles, in the context of hybrid a new dynamic of engagement has emerged. In a situation of perceived urgency, member states of both organisations granted more leeway to staff to improve cooperation and find synergies. This new momentum, in turn, allowed

---

159 Interview with Col. Calaresu, op. cit.
160 European Commission & HR/VP, op. cit., pp. 16-17.
161 Ibid., p. 13.
162 Interview with G. Iklody, op. cit.
163 Ibid.
both organisations to progressively deepen their relationship, despite political blockages. Despite the slow progress of formal EU-NATO cooperation, hybrid set the tone for closer NATO-EU institutional relations. In this respect, the evolution of the unofficial staff-to-staff contacts seems significant, as it paved the way for subsequent developments in EU-NATO cooperation.

A hybrid opportunity

The High Representative, in coordination with the Commission, will continue informal dialogue and enhance cooperation and coordination with NATO on situational awareness, strategic communications, cybersecurity and ‘crisis prevention and response’ to counter hybrid threats, respecting the principles of inclusiveness and autonomy of each organisation’s decision making process.164

The May 2016 EU Foreign Affairs Council conclusions on hybrid threats stressed “that cooperation with NATO had to be at the heart of the EU’s CSDP” [Common Security and Defence Policy].165 The emphasis on cooperation between the two organisations was largely a product of several Ministers’ insistence, pushing for working with NATO especially on the issue of strategic communications in the context of Russian actions in Ukraine.166 The prominence of NATO for the EU in the context of hybrid was also a question of timing. Indeed, there was “a unique opportunity begging” in the fact that “[n]either the EU nor NATO [had] a strategy to counter hybrid threats” and that both could build “complementary and mutually supporting strategies”,167 with the Alliance being seen as “an integral part of [EU] planned actions” on hybrid.168

Closer relations being a key objective for some states like the UK169 or Poland,170 hybrid provided an opportunity to seek “new ways of cooperation”,171 including efforts to strengthen the informal dialogue between the two organisations.172 The leadership and good relationship of NATO’s Secretary General and the EU’s HR/VP proved instrumental for

---

164 European Commission & HR/VP, op. cit., p. 17.
165 House of Commons, Documents considered by the Committee on 9 September 2015, European Scrutiny Committee, London, 2015.
166 Ibid.
167 EEAS (CMPD), op. cit., p. 5.
168 F. Mogherini as quoted in NATO Press Release, Press statements by the NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini, December 2015.
169 House of Commons, op. cit.
171 EEAS (CMPD), op. cit., p. 6.
172 European Commission & HR/VP, op. cit., p. 17.
closer relations. Hybrid also became a priority of the rotating Presidency held by the Netherlands, culminating in the EU-NATO Joint Declaration on the margins of the Warsaw Summit and its subsequent implementation process, the clear majority of the proposals having an explicit or implicit hybrid dimension. In general, the discussion on hybrid threats significantly contributed to further NATO-EU coordination.

Cooperation out of necessity?

The absence of an effective official framework for EU-NATO cooperation has been described by one European Foreign Affairs Minister as “a threat to European security, particularly in the face of hybrid threats”. Similarly, the European Defence Agency (EDA) Chief Executive stated that EU-NATO cooperation on hybrid “is not an option, but an absolute necessity”. These statements point to perceived vulnerabilities in both organisations, from which a generalised feeling of urgency can be inferred, explaining efforts to understand “who does what and when”.

The EDA Chief Executive brought some clarity in this regard, stating that “[t]he deterrence effect of NATO and the complementarity of [EU] tools and instruments, are more than enough reason to enhance our cooperation”. In this vein, the following calculus seems to have emerged, in which “the EU possesses many of the capabilities that NATO does not, [including] the ability to broadly assess Europe’s vulnerabilities, and to produce a ‘risk register’ of areas including critical national infrastructure to help indicate when hybrid actions might be under way”. Indeed, while both the EU and NATO see their member states as the “first responders” on hybrid, “closer cooperation between [both organisations] can make [their] assistance more focused and more effective”.

---

175 Waszczykowski, op. cit.
176 EDA Press Release, Countering Hybrid Threats: ‘Capabilities need to be used in a more coherent and comprehensive manner’ (Jorge Domezcq), 4 March 2016.
177 Stoltenberg as quoted in P. Pemik, EU and NATO: Enhancing Cooperation to Counter Hybrid Threats, European Leadership Network, Online Article, 2015.
This line of thinking was in particular evident concerning topics “related to economic measures, energy, cyber and so on” in which NATO was perceived to need additional means. Cyber in particular has to be viewed as the area in which most has been achieved by both organisations – the signing of a Technical Arrangement by the NATO Computer Incident Response Capability and the EU’s Computer Emergency Response Team in 2016 is a prime example. Hailed by the EEAS as “an important milestone to implement the objectives of the EU Cyber Defence Policy Framework”, the agreement was in fact an institutionalisation of unclassified information exchange, allowing for structured staff-to-staff contacts between the two bodies – a relatively minor development with a symbolic dimension, in an inter-institutional context where “symbols do matter”. Similarly, the prominence of cyber in the process of implementation of the NATO-EU Joint Declaration further illustrates this point.

Indeed, a key dimension of NATO-EU cooperation on hybrid seems to be the very symbolism it can bring to bear in the current crises facing Europe. One such issue with an impact on European public opinion was the migration crisis. Seen as a “key test of relevance” for the Alliance, it led to NATO engaging its naval assets in patrolling the Aegean, exchanging information with the EU’s Frontex through liaison officers, as well as the launch of NATO Operation Sea Guardian to support EUNAVFOR MED in the Mediterranean.

Overall, the process of implementation of the NATO-EU Joint Declaration has to be analysed in the context of discussions on hybrid, while keeping in mind the Cyprus-Turkey issue impeding fully-fledged cooperation between the two institutions. Any new development in interinstitutional cooperation is a product of months of intense negotiations among the two organisations, but also between their constituent bodies and member states, and, in some cases even between individual national ministries. In practice, this means that any development in the official NATO-EU relationship is dwarfed in scope by unofficial interactions which made it happen at the staff level. In this context, it can be said without

181 J. Stoltenberg as quoted in NATO, Pre-ministerial Press Conference by NATO Secretary General Jens Stoltenberg, 11 May 2015.
182 EEAS Press Release, EU and NATO increase information sharing on cyber incidents, 160210_01_EN, 10 February 2016.
183 Ibid.
184 Interview with G. Iklody, op. cit.
185 Interview with J. Shea, op. cit.
186 Baranowski & Lété, op. cit., p. 12.
187 NATO Website, Assistance for the refugee and migrant crisis in Europe, 24 March 2016.
188 Council of the EU, op. cit., p. 3.
doubt that it is the sense of urgency created by hybrid, and especially by Russian actions in Ukraine, which created the “new impetus” in the official EU-NATO relationship.\footnote{Council of the EU, op. cit., p. 2.}

Condemned to unofficial coordination

To counter hybrid in a coordinated fashion, NATO has been engaged in (mostly) unofficial talks with the EU in four different areas: “civil-military planning, cyber-defence, information-sharing and strategic communications”.\footnote{Shea, op. cit., NATO Review.} Several unofficial 28-to-28 meetings took place in early 2016, with intelligence sharing proving the most contentious topic of discussion at the time.\footnote{Interview with anonymous NATO official, op. cit.} These meetings were, however, merely one manifestation of the increasing contacts between the two institutions. Indeed, as noted by Pernik, “the frequency and topic areas of staff-to-staff meetings have grown, both at political and expert levels and the informal cooperation network functions well”.\footnote{Pernik, op. cit.} Equally important, despite blockages on information sharing between the two organisations, as confirmed by several of my interviews, “information is being shared in brown envelopes” and regular staff meetings are being encouraged.\footnote{Interview with G. Iklody, op. cit.}

Another aspect of this unofficial cooperation is linked to COEs. The European Centre for Countering Hybrid Threats, currently being set up in Finland, has the potential to be significant in this respect. Indeed, COEs present the advantage that they “are half-in, half-out” of their institutional setting, which opens possibilities for cooperation with outside partners.\footnote{Ibid.} The planned COE would thus be able to cooperate with all NATO COEs which deal with issues connected to hybrid (such as counterterrorism, cyber, CBRN, energy etc.), thus feeding into coordinated policy responses of both organisations. It remains to be seen though whether this new COE will be doing anything more than “raising awareness from an academic point of view”.\footnote{Interview with Col. Calaresu, op. cit.} On the other hand, the new centre could be an added value, especially if it is set up as more than just an academic institution, on the lines of the more ‘operational’ NATO Cooperative Cyber Defence COE in Estonia.\footnote{Interview with J. Shea, op. cit.}
While some officials still seem to see some sort of a competition between NATO and the EU, most seem to perceive this mind-set as outdated. A related issue is to what extent the levels of unofficial cooperation are sustainable and themselves resilient against hybrid. As stated by one NATO official, both the Union and the Alliance “would like to see a more organised way of doing it [but] both organisations first need to sort themselves out internally”. A similar picture has been presented to me by an EU official, who stated that the hybrid discussion had the potential of having a positive impact on intra-EU coordination, which so far is “almost non-existent”. Despite limited developments in official NATO-EU cooperation in 2016/17, the conclusion for now still seems to be that the status quo remains the rule.

To conclude, it can be said that the current levels of EU-NATO cooperation are largely a product of the hybrid threat context. While both official high-level and unofficial staff contacts have increased, most cooperation arrangements remain ad hoc and limited to certain policy areas carefully negotiated by member states of both organisations and the organisations themselves. On the other hand, changing staff mind-sets in both organisations, slowly push new synergies to the surface, as well as crystallising relationships and working methods, which have the potential to outlive the hybrid terminology.

Conclusion

Hybrid has been around for a decade, gradually transforming and diffusing across the Atlantic. In doing so, it could give the impression that “perhaps the most successful manifestation of hybrid warfare, [was] the confusion it caused in terms of our vocabulary”. In my opinion, the emergence and persistence of the hybrid terminology points to the demand for new ways to describe what some see as novel challenges. To a certain extent, the progressive dilution of the meaning of this terminology is the result of similarly elusive processes to those it seeks to describe. Hybrid should be seen as a manifestation of an inability to fit current security challenges within previously delineated schemata for conceiving war. Indeed, by virtue of its diffusion in policy-making and expert communities, in

197 Interview with anonymous EU official, op. cit.
198 Various interviews.
199 Interview with A. Budd, op. cit.
200 Interview with G. Iklody, op. cit.
201 Interview with anonymous NATO member state diplomat, op. cit.
particular via NATO, the malleable term became the canvass upon which different institutional actors and nations could project their threat perceptions.

Through extensive research, I have shown that hybrid war and hybrid threats have been deduced by ‘looking in the mirror’ – thus being a product of self-diagnosed vulnerabilities. It is precisely this perception and the vague nature of this terminology, which led both NATO and the EU to adapt hybrid to describe a changing security environment to which no clear policy responses existed. The need for a novel concept points to a growing realisation that Western models of war and peace were inadequate to describe a rapidly evolving strategic international environment. As such, the hybrid label is not about Russia or the Islamic State, but rather seeks to communicate a state of urgency at a time of nominal peace.

While perceptions of what hybrid is differ within NATO and the EU, there seems to be a growing consensus that both organisations need to adapt. A perception of vulnerability and a sense of urgency is what led both organisations to seek synergies in their respective policy responses, resulting in a qualitative change in their informal staff-to-staff interactions, and ultimately, in increased formal NATO-EU cooperation. Hybrid was a useful concept for both organisations, vague enough to secure the buy-in of all NATO and EU member states, and to facilitate EU-NATO communication despite the lack of precise agreement on what hybrid means.

No clear-cut definitions and categorisations are needed to understand that the West lags behind in adapting to a networked security environment, where power is more diffused on all levels. Seeing the patterns is easy, starting to adapt is harder, but the real challenge is to communicate these changes to decision-makers and populations. In this sense, hybrid was a useful communication tool, but its inherent vagueness carries the risk of suboptimal policy outcomes, especially when policy-makers, media, think tanks and politicians start using this terminology in disparate ways.

While the EU deliberately chose hybrid threats over hybrid warfare to emphasise a ‘comprehensive’ response mostly anchored in its civilian nature, NATO concentrated on showcasing Allied solidarity and putting more emphasis on projecting stability outside its borders. I have nonetheless shown that in both cases, the hybrid terminology has almost not altered the EU or NATO internal processes and policy proposals. What it did achieve, was pushing existing adaptation programmes to the top of the agenda, showcasing internal
inadequacies and the need for both organisations to work closer together. All in all, despite its flaws, hybrid brought NATO and the EU closer together in challenging times.
Bibliography


Council of the EU, Hybrid Threats, YouTube, 18 April 2016, retrieved 19 April 2016 [https://www.youtube.com/watch?v=SPs9DYjY35s]

Council of the EU, Council Conclusions on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, 15283/16, 6 December 2016, pp. 1-11.


House of Commons European Scrutiny Committee, Documents considered by the Committee on 9 September 2015, retrieved 31 March 2017 [http://publications.parliament.uk/pa/cm201516/cmselect/cmeuleg/342-iii/34209.htm]


Miklaucic, Michael, NATO Countering the Hybrid Threat, NATO ACT, 23 September 2011, retrieved 31 March 2017 [http://www.act.nato.int/nato-countering-the-hybrid-threat]


NATO StratCom COE, Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia, Riga, 2016, pp. 1-106


USJFCOM, Irregular Adversaries and Hybrid Threats, Joint Irregular Warfare Center, 2011, pp. 1-33 [https://info.publicintelligence.net/USJFCOM-IrregularThreats.pdf]


**Interviews**

Interview with Andrew Budd, Head, Defence Capabilities Section, Defence Policy and Planning Division, NATO, via telephone, 4 April 2016.

Interview with anonymous EU official, Brussels, April 2016.

Interview with anonymous NATO Member State diplomat, Brussels, April 2016.

Interview with anonymous NATO official, Brussels, April 2016.

Interview with Axel Butenschoen, Project Officer for Capability Development Plan, European Defence Agency, 7 April 2016, Brussels.

Interview with Colonel Sandro Calaresu, Military Assistant, CMPD, Brussels, 14 March 2016.

Interview with Dr. Jamie Shea, Deputy Assistant Secretary General for Emerging Security Challenges, NATO, via telephone, 31 March 2016.

Interview with Dr. Patrick Cullen, Senior Research Fellow, NUPI, via telephone, 8 April 2016.

Interview with Mr. Gabor Iklody, Director of CMPD, EEAS, Brussels, 21 March 2016.

Interview with Prof. Dr. Sven Biscop, Director Egmont Institute, Bruges, 9 March 2016.

**Conferences**

Conference remarks of an anonymous European Commission official, Bruges, April 2016.

List of recent EU Diplomacy Papers

For the full list of papers and free download, please visit www.coleurope.eu/EDUP

1/2016
Hugh O’Donnell, The European Union as a Mediator in Israel-Palestine: Operations Cast Lead and Protective Edge

2/2016
Michal Ovádek, External Judicial Review and Fundamental Rights in the EU: A Place in the Sun for the Court of Justice

3/2016
Michaela Anna Šimáková, The European Union in the OSCE in the Light of the Ukrainian Crisis: Trading Actomess for Effectiveness?

4/2016
Donal Kennedy, Between Sisyphus and the Danaïdes? The European Union’s Efforts to Promote and Protect the Human Rights of LGBTI Persons in its Eastern Neighbourhood

5/2016
Thomas Jacobs, The Language Diplomats Speak: A Discourse-theoretical Approach to the Negotiations in the EURONEST Parliamentary Assembly

6/2016
Paloma Díaz Topete, ‘Pastis Power Europe’: An Assessment of the EU’s Actomess in International Investment Politics

7/2016
Aurore Loste, ‘Békou’, le fonds fiduciaire de l’Union européenne pour la République centrafricaine: un espoir pour le financement des Etats fragiles en transition ?

8/2016
Matteo Ricci, The European Air Transport Command: A Viable Model for Promoting European Military Cooperation?

1/2017
Thomas Coibion, How Effective Is the EU as a Mediator? The Case of the Former Yugoslav Republic of Macedonia

2/2017
Marikki Rieppola, The EU Advisory Mission Ukraine: Normative or Strategic Objectives?

3/2017
Martin Ronceray, A Bureaucratic Bias? EU Election Observation Missions in Africa: Between Independence and Development Industry

4/2017
Benedikt van den Boom, EU Region-Building in the Neighbourhood: The Eastern Partnership’s Contribution in the South Caucasus

5/2017
Jan Jakub Uziębło, United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats


