Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO

Maria Mälksoo

Routledge
Taylor & Francis Group

Check for updates

Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO

Maria Mälksoo [a,b]

aBrussels School of International Studies, University of Kent, Brussels, Belgium; bEspace Rolin, Brussels, Belgium

ABSTRACT

What are the ethical pitfalls of countering hybrid warfare? This article proposes an ontological security-inspired reading of the EU and NATO's engagement with hybrid threats. It illustrates how hybrid threat management collapses their daily security struggles into ontological security management exercise. This has major consequences for defining the threshold of an Article 5 attack and the related response for NATO, and the maintenance of a particular symbolic order and identity narrative for the EU. The institutionalisation of hybrid threat counteraction emerges as a routinisation strategy to cope with the "known unknowns". Fostering resilience points at the problematic prospect of compromising the fuzzy distinction between politics and war: the logic of hybrid conflicts presumes that all politics could be reduced to a potential build-up phase for a full-blown confrontation. Efficient hybrid threat management faces the central paradox of militant democracy whereby the very attempt to defend democracy might harm it.

Introduction

A spectre is haunting the Western world – the spectre of hybrid warfare. All threats "hybrid" have become the buzzword of the international security commentariat ever since Russia's swift annexation of Crimea in 2014 with the help of the "little polite green men"[1] and Russia's involvement in the ongoing conflict in eastern Ukraine. The allegedly Kremlin-led meddling in the US presidential elections of 2016 is the most recent high-profile episode in this sequence of low-intensity "political warfare", described by Mark Galeotti (2016b) as a "21st century conflict, more Machiavellian than military, where hacks, leaks and fake news are taking the place of planes, bombs and missiles". Similar destabilisation campaigns have been noticed in the context of the French presidential election and in the build-up to German federal elections in 2017, and in numerous other European states.[2]

While the "new wars" debate has a long pedigree in international studies (Kaldor 1999, 2013, Henderson and Singer 2002, Evans 2003, Newman 2004, Smith 2005, Hoffman 2007, Münkler 2005, Strachan and Scheipers 2011), the scholarship has remained largely silent

---

on the potential of these wars to generate immaterial insecurity effects. This article offers an ontological security-situated reading on the added insights the notion "hybrid warfare" brings to bear for our understanding of the contemporary Western security predicament. Ontological security (OS) is a condition underpinning the actor's ability to act in the world with basic confidence about how the world works and her own place within it.[3] Ontological insecurity, in turn, signifies "the deep, incapacitating state of not knowing how to get by in the world" (Mitzen and Schweller 2011, p. 29). With an explicit emphasis on uncertainty and anxiety as the key referents in ontological (in)security, this contribution seeks to complement the literature on the changing character of war by illuminating the disturbing ripple effect of hybrid warfare not only for the central security-political organisations of the West, but also for the ontological underpinnings of the International Relations (IR) discipline more generally.

I propose to link the study of OS in IR systematically with the debates on hybrid warfare along ontological, epistemological, and ethical dimensions to provide sharpened analytical purchase for understanding the nature of, and the emerging Western responses to, the said challenge. An OS perspective brings to the generally policy-centric study of hybrid threat management a systematic and conceptually rigorous understanding of the dual dynamic of anxiety (as a sense of unease and uncertainty), and routinised practices (as modes to confront anxiety in order to provide a stable cognitive environment) with important ethical and legal implications for conceptualising war (see Mitzen 2006, p. 346). My main argument is that "hybrid warfare" capsizes an embedded cognitive structure about what war is, thus defying attempts of organising life and social relations in a particular way, with fundamental consequences for the OS of the European Union (EU) and NATO. I proceed from the premise that defending and promoting a particular vision of one's self is important for the "security of being" of these Western security-political institutions, and a prerequisite for the strategic use of their agency (Flockhart 2016, p. 801). This article offers an exploration of the EU and NATO's identity maintenance "especially by acting, or doing things" (Mitzen and Schweller 2011, p. 28) vis-à-vis hybrid threats. It thus subscribes to Flockhart's suggestion that the two strategies of OS maximisation (a "strategy of being" and a "strategy of doing") are interlinked and cannot be understood in isolation from one another (Flockhart 2016, p. 799, p. 816).

What authority claims are the EU and NATO making about their ability and competence to handle hybrid challenges, or the "new type of warfare"? What is the "security story" these bodies articulate, accordingly? How are their respective attempts of countering "hybrid threats" embedded in particular understandings of politics and war? What signs of discursive cross-pollination can we observe comparing the two organisations in their hybrid threat/warfare management strategies and practices? How does it all relate to their respective identity sustenance struggles?

Below, I set out to show how the hybrid war discourse epitomises the contemporary ontological insecurities of the EU and NATO. Attempts to frame bold institutional responses to the "hybrid" threats, notably via the promotion of resilience as the institutional equivalent of a sense of OS, mark "bringing the war back in" for the international security management profiles of these two major Western organisations. NATO and the EU's emerging discourse and practice in countering hybrid warfare seek to prove their continuing relevance in the contemporary era. The preoccupation with hybrid threats has made the concept of war empirically more available for the EU. Albeit war continues

to be normatively unacceptable, public discussion of concrete practices to counter various "hybrid" moves from third parties as part of the broader "hybrid warfare" countering paradigm is far from a taboo for the EU in this day and age.[4] NATO as a more traditional security organisation is wrestling harder with the threshold of war becoming increasingly fluid in the context of "hybrid" engagements. Lawyers debate whether "hybrid warfare" calls for updates in the law of armed conflict. Ultimately, it is the legal characterisation which determines whether a situation is considered to amount to armed conflict, and accordingly, whether peacetime law or law of war applies (O'Connell 2015). The hybridisation of warfare further challenges the (substantively anyway dubious) legal distinction between international and non-international armed conflicts (Reeves 2016). Meanwhile, the general acceptance of the term "hybrid war(fare)" also signals the politicisation of the established legal definition of war as a particular practice that takes place when certain specific conditions have been fulfilled.

Brandishing "war" on political contestations of varying intensity has furthermore ethical implications (cf. Franke 2015). As the EU and NATO are grappling with honing their response to the menaces and tactics combining a mixture of special forces, backdoor proxies, information campaigns, and "digital warfare" (e.g. Ilves 2016), having further added the non-state variant of the "hybrid threat" to the mix (such as Daesh), a broader question transpires about the repercussions of the alleged hybridisation of warfare and its perpetrators for the study of security in IR.

The article proceeds in four sections. The first section gauges various definitions of hybrid warfare, outlines their relation to the notion of ontological insecurity, and the consequent countering attempts of hybrid threats to the mirror-image process of OS-seeking. I make a threefold proposition: hybrid warfare is disturbing *ontologically*, because it embodies the entanglement of politics and war in the contemporary era; *epistemologically*, because it unhinges the war/peace binary implicitly underpinning the IR discipline (Barkawi 2016);[5] and last but not least *ethically*, because the inherent danger of becoming a monster in the course of fighting monsters (aka the efficient countering of hybrid warfare) is particularly poignant for democratic polities (cf. Nietzsche 2003, Aphorism 146). The second section applies various OS-attuned lenses on the institutional responses of the EU and NATO to hybrid warfare, and the third section empirically illustrates the argument. The article concludes with a call for caution: adopting the "everything is dangerous"-approach further blurs the fuzzy line between politics and war, adding heat to the calls to revisit the international laws on armed conflicts (cf. Winter 2011). The justifiability of illiberal methods in safeguarding liberal values constitutes the crux of the OS dilemma for the Western security community battling the "hybrid menace".

Hybrid warfare as the epitome of ontological insecurity

Much of the strategic studies literature has been animated by the problem of uncertainty in international relations and, by extension, the consequences of uncertainty for the management of states' security dilemma (Rathbun 2007, cf. Mitzen and Schweller 2011). Ambiguity is likewise the original sin the "hybrid warfare"-notion draws on. Yet, the concept "hybrid warfare" is itself faulty of definitional ambiguities. Although an increasingly utilised concept in the contemporary strategic and policy discourse, "hybrid warfare" refers to a number of distinct phenomena, and consequently means different things to different

people. It lacks a clear and uniform definition, hence embodying and perpetuating the countenance it seeks to capture. "Hybrid warfare" is thus victim to its own conceptual plasticity (Tenenbaum 2015, p. 43).

The heterogeneous origins, composition, and use of the concept can be somewhat clarified by distinguishing between (i) hybrid *threats* (as complex and multidimensional modern menaces, crisscrossing multiple issue areas and amplifying one another); (ii) hybrid *warfare* (as a particular mode of waging war, combining conventional and unconventional, coercive and non-coercive means, capabilities, tactics and formations in a centrally organised and orchestrated manner), and (iii) hybrid *war* (as "a form of violent conflict that simultaneously involves state and non-state actors, with the use of conventional and unconventional means of warfare that are not limited to the battlefield or a particular physical territory" (Jacobs and Lasconjarias 2015, p. 3, cf. Jonsson and Seely 2015, Browning 2002, p. 2). Tenenbaum (2015) offers a useful genealogy of the "hybrid warfare" concept, highlighting the notion's distinct effects at the political and strategic, operational, tactical and capability levels. Yet, the practical use of the term "hybrid" has interchangeably and rather confusingly moved between these different levels of analysis, seeking to capture the interconnected nature of modern vulnerabilities, the multiplicity of stakeholders in the contemporary security game (i.e. state and non-state actors, regular and irregular forces), along with the diversity and simultaneity of conventional and unconventional means used, ranging from military, political, economic, diplomatic, technological to criminal modes of engagement (Hoffman 2007, Glenn 2009, Pawlak 2015). Writings on hybrid warfare thus tap into both the literature on asymmetric/counterinsurgency warfare (McCuen 2008, cf. Winter 2011) and that on interstate wars (Gerasimov 2013). No wonder that "hybrid" has come to accommodate as varied phenomena as Russia's takeover of Crimea in 2014 and its involvement in the ongoing conflict in eastern Ukraine, Russia's meddling in the elections of various countries around the world via sophisticated phishing, doxing, and fake news campaigns, and the regional and global operating logics of politically ambitious non-state organisations, such as Hezbollah, Boko Haram, Al-Qaeda, or Daesh, or even criminal structures (e.g. the drug cartels in Mexico; see further Tenenbaum 2015).

Drawing on the emerging scholarship on hybrid warfare, three core interconnections can be flagged between hybrid warfare (as an empirical phenomenon and a discursive trope) and (the study of) OS in IR. First, along the *ontological dimension*, "hybrid warfare" captures the increasing porousness of lines between politics and war in the contemporary era, thus defying the attempts of organising life and social relations in a particular way (cf. Huysmans 1998). While many critics of the notion maintain that hybrid warfare remains just another variation on the old Clausewitzian understanding of war as the continuation of politics with a mixture of other means (cf. Gray 2007), others nonetheless highlight the particularity of the contemporary hybrid engagements. For the scholars finding distinct added value in the notion, the calibration and central coordination of the convergence of the various regular and irregular elements, further amplified by the new technological vulnerabilities and capabilities in contemporary hybrid engagements, have made the creeping indeterminacy about *what* war exactly is and *how* to go about it in the present day only more intense. The envisioning of hybrid engagements as a pre-phase of a full-scale military attack further adds to the ambiguity between the

boundaries of warfare as essentially organised, reciprocal fighting and politics as a peaceful space of ordinary goings-about.

For those at the receiving end, hybrid warfare emerges as an epitome of ontological *in*security, referring to the "deep, incapacitating state of not knowing which dangers to confront and which to ignore, i.e. how to get by in the world" (Mitzen 2006, p. 345). It is an urgent reminder of the chameleon-like character of war – that is, war's tendency to constantly change its forms as well as its appearances (Clausewitz 1976, p. 80). At the most fundamental level, then, hybrid warfare epitomises the blurry line between politics and war. It also symbolises the struggle for, and fear over losing, control "over the ends, ways and means of nations, communities and societies" (Ruiz Palmer 2015, p. 61). Assuming that collectivities' agency is predicated on identification and routinisation (Greve 2017, p. 7), uncertainty about the nature of external threats does not just generate physical insecurity but also evokes ontological insecurity for the institutions (such as military) and organisations in question. Hybrid warfare exposes collective actors to the fundamental existential questions about the continuity of their external environment as they know it and their own finitude, with the related anxiety about the difficulties of concretising unknown and indeterminate threats (cf. Ejdus 2017). Thus formulated, hybrid warfare directly targets actors' "security of being" (Kinnvall 2004, p. 746), disturbing the stability of their sense-making attempts of the surrounding world and the events they are faced with, and threatening to unsettle the established institutionalised routines. Instead, hybrid warfare itself emerges as an "institutionalization of doubt", provoking considerable ontological insecurity (cf. Giddens 1990, pp. 92–94).

Epistemologically, and on a second note, "hybrid warfare" thus significantly unsettles the "war/peace binary" which has arguably structured the thinking about, and categorisation of, war in the Eurocentric tradition of its study. This particular understanding of war(time), cleanly juxtaposed to peace(time) has been attuned to the needs of an international system of sovereign nation-states, enabling the consequent categorisation of war into international (inter-state) and civil (intra-state) war (Barkawi 2016). "Hybrid wars" emphatically challenge a neat war/peace binary, which has, however, served as a core source of OS for the discipline of IR. There is a family resemblance between the concepts of "hybrid warfare" and the notion of "unpeace" introduced by Kello (2017), seeking to capture the ambiguous, yet persistent irritants by virtual weapons on the international order.

Finally, hybrid warfare meets OS at the intersection of *ethical security studies* (Browning 2016, Browning and McDonald 2013). Just as OS-seeking practices need to be analysed with an eye on the ethical conundrums and dilemmas they might give rise to due to the exercise of power along the way (e.g. Mälksoo 2015, Rossdale 2015), the "social turn" accompanying the hybridisation of warfare in various empirical settings, and the consequent countering attempts of hybrid warfare, require equally intent ethical attention (see Owens 2012). If hybrid conflicts are understood as full spectrum wars … combining a struggle against an armed enemy and a wider struggle for, control and support of the combat zone's indigenous population, the support of the home fronts of the intervening nations, and the support of the international community (McCuen 2008, p. 108), hybrid warfare really appears as yet another variation on the theme of "war amongst the people". The intermingling of political and military activities thus not only underscores the need for their parallel examination (Smith 2005), but also calls for caution in the lax use of war as a metaphor for engagements of various types and intensity. If society

must be defended (Foucault 2003) against nearly everything, at all times, and if everyone becomes connected and potentially targeted in the global "hybrid war" zone, what is left of politics, and the delicate balancing act between security and democratic liberties? The implications of constant public perception management in the service of protecting the freedom of speech in the "post-truth" world are perhaps not fully fathomable yet. The disconcerting potential of the increasingly prominent strategic communication discourse in the EU[6] and NATO[7] for the everyday of democratic politics is already evident (cf. Garton Ash 2016). Securing a core democratic value – freedom of speech/freedom of media – via an obsessive emphasis on proactive and purposeful communication management points at the classic paradox of militant democracy whereby the very attempt to defend democracy might inadvertently damage it (cf. Müller 2016, p. 253).

Managing hybrid warfare as ontological security-seeking

Hybrid warfare emerges as the embodiment of uncertainty for the EU and NATO. The meanings of uncertainty range from fear, ignorance, confusion, and/or indeterminacy in IR theory (Rathbun 2007, pp. 533–534). It is certainly possible to apply all these lenses and consequent emphases on reading the EU and NATO responses to the fundamentally undetermined condition of hybrid warfare, ambivalence *par excellence*. Paraphrasing Huysmans's (1998) original application of the OS concept in IR, the Western countering attempts of hybrid warfare tell a security story wherein a fear of uncertainty, or of the unknown trumps a more concrete fear of death at the hands of other people. As hybrid warfare vividly symbolises "an epistemological fear – a fear of not knowing" (Huysmans 1998, p. 235) (e.g. when war is waged at "us"; what is this "new" kind of "war" really all about etc.), the emerging strategic responses of these two core Western organisations demonstrate how the double fear of death and not knowing quite when and in which ways to expect it, gets objectified in order to make the growing list of potentially existentially dangerous subjects and phenomena more concrete, palpable and conceivable for oneself. Hybrid warfare thus emerges as the "unbearable void" (Huysmans 1998, p. 237), which needs to be objectified, in order to become "knowable" and (more) tolerable.

Huysmans (1998) defines OS as a strategy for managing the limits of reflexivity by fixing social relations into a symbolic and institutional order. In his interpretation, OS thus concerns the general question of the political, or "how to order social relations while simultaneously guaranteeing the very activity of ordering itself" (Huysmans 1998, p. 242). Hybrid warfare, by definition, destabilises the traditional cognitive security environment of states and international organisations, and consequently, renders their identity insecure. Crafting the institutional responses to hybrid warfare thus becomes a "dread management" exercise wherein daily security administration attempts, seeking to objectify the abstract fear of death through constructing concrete enemies and thus introducing a level of certainty, nonetheless remain toothless at the inability to "hierarchize threats" in an atmosphere of potentially permanent state of crisis and urgency (Huysmans 1998, p. 243). The pursuits of daily security and OS ("security of being") thus collapse into each other.

Hybrid warfare indicates a multitude of possible contingencies, generating anxiety about one's ability to remain oneself and to continue to act. It is thus linked to "anxiety over the vulnerability of [Western] power" (Bell 2012, pp. 230–231), threatening the West about losing its particularistic form of existence (cf. Creppell 2011, p. 455). Anxiety, in contrast to

fear, which per Giddens (1991, p. 43) constitutes a response to a specific threat, concerns "perceived threats to the integrity of the security system of the individual" (Giddens 1991, pp. 44–45, cf. Browning and Joenniemi 2017, p. 38; Rumelili 2015). OS-seeking aims to mitigate the effects of such hard uncertainty, bringing it within bearable limits (Mitzen 2006, p. 346). Routines are instrumental here, as they "pacify the cognitive environment … 'inoculating' individuals against paralytic, deep fear of chaos" (Mitzen 2006, p. 347).

Being able to survive the "hybrid threats" is directly pertinent to the survival of the EU and NATO as particular kinds of organisations, underpinned and driven by specific values – which cannot be sacrificed or diluted in the struggle for physical and institutional survival. Yet, hybrid warfare disturbs the OS of the EU and NATO in subtly distinct ways. Due to the particularities of their institutional set-ups and historical foundations, the OS drives of the two organisations are somewhat distinctive. NATO's history is occasionally told through its surpassing of a sequence of crises, albeit the end of the Cold War and the collapse of its original enemy created a situation of unprecedented uncertainty and ontological insecurity for the Alliance. Meanwhile, the EU's ontological insecurity is a more recent phenomenon, stemming mostly from the Eurocrisis and the looming possibility of a Grexit a few years ago; the refugee/migration crisis in Europe of 2015 (Dingott Alkhoper 2018; Mitzen 2018); the actual UK decision on Brexit in 2016 (Browning 2018); and the rise of populist politics within the EU (Kinnvall, Manners, Mitzen 2018) and the United States. NATO as a military alliance has been historically more accustomed to the othering practices of concrete geographical places, whereas the EU is generally regarded as an organisation that has risen above geopolitical othering, juxtaposing itself to Europe's dark past instead (Rumelili 2018, Subotic 2018, and Della Sala 2018). Accordingly, the EU might be more at home with hybrid threat management due to its historically broader conceptualisation of security through the paradigm of intertwined risks rather than being focused more strictly on "the threat, use and control of military force" in the manner of a traditional defence alliance (Walt 1991, p. 212; Manners 2002). Regardless of its perpetual transformer's self-image, hybrid threats represent the uncomfortable "hard" or "fundamental" uncertainty for NATO (cf. Mitzen 2006, p. 346) and are thus ontologically disturbing for the security of its self as a traditional alliance with a collective security pledge bound to "armed attack" against one or more of its member states.

In order to achieve OS, actors strive for "routinizing their relations with significant others" (Mitzen 2006, p. 342). Routines help to keep ontological fears at bay, out of everyday discursive consciousness (Mitzen 2006, p. 348). From this perspective, NATO's naming and shaming strategy vis-à-vis Russia as part of its hybrid warfare countering strategy links the uncertainty emanating from the hybrid nature of the new threats to the known and routine relationship with its traditional antagonist.[8] The incapacitating difficulties related to planning ahead in anticipating and countering hybrid engagements are thus somewhat alleviated by the latter's attachment to a known rival. Russia's hybrid intervention in Ukraine has concurrently provided NATO with the familiar parameters of the cognitive "cocoon" (Giddens 1991, pp. 39–40) which enables the alliance to reproduce its cognitively "knowable" world. A Mitzenian reading of NATO's emerging response to hybrid threats/warfare thus points at the renewed routinisation of the "programmed cognitive and behavioral responses" to Russia as the alliance's original nemesis.

Restoring traditional vigilance vis-à-vis Russia, buttressing the forward defence along the Alliance's eastern flank with the respective military reinforcements, contingency

planning and exercises, the emerging response of NATO to the hybrid menace could also be read as an attempted restoration of a known normative order for the North Atlantic Alliance. Hybrid warfare endangers the basic features of the said normative order (or that of the broadly conceived Western security community in general, including the EU as well) as its efficient countering would likely compromise the underlying principles for this order's particularistic existence (cf. Creppell 2011, p. 450). As a threat of subversion, hybrid warfare exposes the internal vulnerabilities in the body of the traditional security alliance (NATO) and a self-proclaimed post-modern security actor (i.e. the EU; cf. Cooper 2004). This concerns, in particular, the ever-elusive (and contested) balance between national/organisational security and individual liberties (cf. Waldron 2003, Neocleous 2007), as strategic communication is inherently at odds with free speech as a core value of Western liberalism. Countering hybrid warfare is conducive of generating a security predicament of perpetual pre-emption which, by definition, would indicate pre-emptive gathering of all sorts of data, thus likely infringing on the privacy of the individuals for the sake of the organisational/regional/national security. This precautionary logic resonates with the risk society approach which characterises the struggling with a sheer volume of risks with potentially fundamental consequences as a key feature of modernity, implying that "decisions are … made not in context of certainty, nor even of available knowledge, but of doubt, premonition, foreboding, challenge, mistrust, fear, and anxiety" (Ewald 2002, p. 294).

A less sympathetic reading of such an ontological "dread management" exercise would regard particularly NATO's emerging narrative and practice about hybrid warfare as an example of turning unknown anxieties into "the manageable certainties of objects of fear to physical security through securitization" (Browning and Joenniemi 2017, p. 38, Rumelili 2015, Steele 2008, p. 64). NATO's and the EU's "dread management" strategies vis-à-vis the hybrid "spectre" tune us further in the direction of Croft and Vaughan-Williams's (2017, p. 27) research agenda, asking specifically "[w]hose dread is managed and at what cost for whom?", thus illuminating the ethical pitfalls related to their OS-seeking. Due to the omnipresence and ambivalence of hybrid threats, NATO and the EU's countering strategies of hybrid warfare verge on "deep securitization", which Abulof (2014, p. 397) defines by its distinctly high scale and scope of securitising moves. The hybrid warfare discourse has become ubiquitous in the respective repertoires of the EU and NATO, with hybrid threats framed as imminent, protracted, and existentially endangering. Securitisation thus emerges as a response to the ontological insecurity, with a promise of "mitigating the existential angst arising from death being both certain and undetermined" (Abulof 2014, p. 403, Huysmans 1998). Both NATO and the EU are engaged in collective securitisation of hybrid warfare since the threat in question has a systemic referent – that is, it "imping[es] upon international and collective identities, or the rules and norms governing interstate interactions" (Sperling and Webber 2017, p. 26). Hybrid threat management by the EU and NATO could accordingly be understood as the institutionalisation of their respective organisational OS-seeking via strategies of "being" (aimed at constructing a strong narrative to buttress a continuous and esteem-boosting identity) and "doing" (focused on an attempt to uphold a stable cognitive environment through routinised practice "whilst also undertaking action contributing to a sense of integrity and pride") (Flockhart 2016, p. 799). While the EU is emphatically defending core democratic values (freedom of expression, freedom of assembly, media

freedom and access to information) (European Parliament 2016), NATO's countering of hybrid threats demonstrates more explicitly the intertwining of its physical survival as an efficient political-military alliance and a sense of OS as the principal warden of the European security (and more broadly Western world) order. The inability to honour the collective defence pledge would be a blow to NATO's identity *and* mean its (almost certain) death. The security of its "body" (i.e. physical security) and "self" (i.e. ontological/identity security) are therefore less distinguishable than in the case of the EU which is a far more complex political setting, with only relatively recent claims (albeit with increasing assertiveness) in the traditional security sphere.[9] Regardless, for both organisations, countering hybrid threats serves as a reactive self-legitimation as they thus reassert their relevance and ability to be of assistance for their respective member states and populations.

Hybrid warfare in daily security management

A bird's-eye view of the EU and NATO's emerging management strategies of hybrid warfare demonstrates how the looming hybrid agenda is directly tapping into the everyday security concerns of these two main Western political and security organisations.

In NATO and the EU's responses to hybrid threats, OS emerges as the actor's ability to tolerate, and cope with change (Browning and Joenniemi 2017, p. 32). Albeit seemingly counterintuitive due to the general human preference for stability over change, OS might nonetheless "derive[] from constructive attempts to (re)create and consolidate collective self-identities" (Vieira 2016, p. 292). The leitmotif of adapting to changing circumstances is reflected in both the EU and NATO's notable emphases on resilience – which, I argue, could be regarded as an institutional alias for their positive sense of self, and by consequence a functional equivalent of these actors' OS. Rendered as "the ability of states and societies to reform, thus withstanding and recovering from internal and external crisis" (Wagner and Anholt 2016, p. 414), "resilience" manifests a claim on a sense of institutional self-worth and relevance amidst deep uncertainty. Invoking "resilience" appears emphatically as an anxiety management rather than avoidance exercise, at relatively low ontological costs involved for the actors concerned. Resilience is thus conceptually linked, yet not synonymous with OS: it functions as an imperfect solution to the perennial ontological insecurity problem – for OS remains always to be measured in degrees, rather than being categorically achievable in practice. As a notoriously flexible notion, politically convenient and intellectually perplexing in equal doses, resilience refers to "the process of seeking to maintain the status quo in the face of shocks, but it also refers [to] the idea of transforming a referent object" (Bourbeau and Ryan 2018, p. 223).

Adaptability, or the ability to cope with change, has been the key trope in NATO's discursive self-presentation throughout the post-Cold War era (Barany and Rauchhaus 2011). Likewise, the EU Global Strategy on foreign and security policy (2016) demonstrates the Union's shift in emphasising "resilience" over more progressive foreign policy goals, as reflected in the earlier, 2003 EU Security Strategy (Mälksoo 2016, Wagner and Anholt 2016, Juncos 2017). NATO and the EU's institutional emphasis on resilience captures the paradoxical dynamic of the "strategy of doing" in their OS maximisation attempts, combining a continuous struggle to manage emergent change by routinised practices, yet also demonstrating ability to undertake action to tackle

transformative change (see Flockhart 2016, p. 816). For what it is worth, "resilience" functions as a symbolic codename for the EU and NATO's institutional responses to the deeply unsettling ontological insecurity condition evoked by hybrid threats/warfare. It captures the necessarily "hybrid" defence to effectively counter the menace in question, including such non-traditional issues as social and political cohesion, vigilance about the funding sources of domestic political parties, and legitimate and effective governance in its spectrum of security (Galeotti 2015, 2016a). Countering hybrid threats by propping the EU and NATO's resilience in various areas (ranging from critical infrastructure, energy and cyber security to transport, financial system and society as a whole) enables a host of claims on the pertinent polities' viability, ability to adjust to the quickly changing demands of the modern world, ownership of the contemporary security scene, and last but not least a workable partnership between the two organisations. Understood "as a preventive and deterrent action to solidify societies and avoid escalation of crises both within and outside the EU" (European Commission 2017), resilience, and the calls to strengthen it, put the main responsibility to the respective member states and their populace, but notably also partner countries in neighbourhood regions (European Commission and High Representative 2017). The vernacular targets of hybrid threats thus become the main stakeholders in the OS management pursuits of these Western organisations, effectively enabling the EU and NATO's evasion of responsibility under the banner of sought OS provision.

The EU

In the EU's official discourse, "hybrid" functions as a catch-all umbrella term, enabling to join concerns about and the related resilience-building activities against Islamic "radicalisation" and "violent extremism" with lessons learned from the Russian actions in Ukraine in recent years. The two leitmotifs of the EU's discourse and emerging practice on countering "hybrid threats" are strategic communication and resilience, with prevention, crisis response, and recovering from hybrid threats acting as supplementary goals. "Resilience" is defined in the Union's Joint Framework on countering hybrid threats as "the capacity to withstand stress and recover, strengthened from challenges" (EU 2016, p. 5). This Framework is designed to "foster the resilience of the EU and Member States, as well as partners" (EU 2016, p. 2). The document defines hybrid threats as

> the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), 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. (EU 2016, p. 2)

The Framework thus refrains from explicitly using the notion "hybrid warfare", discussing instead the appropriate response to "hybrid threats" in the framework of the EU's crisis management, mutual solidarity clause, the Common Security and Defence Policy (CSDP), and in the Union's cooperation with NATO (but cf. EEAS (2015) 731, point 6, p. 2). The avoidance of the explicit "warfare" trope in the EU's policy framework is also evocative of the Union's attempt to sustain the basic continuity with its foundational self-narrative as an antipode to war. It is further symptomatic of the EU's tendency to approach conflict from the perspective of crisis management.

The EU puts primary responsibility in countering hybrid threats to its member states, "as most national vulnerabilities are country-specific" (EU 2016, p. 2). Its own role is envisioned for a coordinated response in order "to build on European solidarity, mutual assistance and the full potential of the Lisbon Treaty" (EU 2016, p. 2). The EU's "key value-adding role" is accordingly deemed to lie in "building awareness" (EU 2016, p. 2). The ambition to gain epistemological control over the hybrid threats spectrum via awareness-raising is supposed "to improve the resilience of Member States to respond to common threats" in turn (EU 2016, p. 2). The resilience-building effort includes the protection of critical infrastructure; adapting and developing necessary defence capabilities; protecting public health and food security; improving cybersecurity in various spheres; targeting hybrid threat financing; countering radicalisation and violent extremism; increasing cooperation with third countries (EU 2016, pp. 5–15). For building societal resilience, a sound strategic communication strategy, making full use of both the new and old media tools, is outlined in the Framework as a core necessity (pp. 4–5). The EU set up the EEAS's East StratCom Task Force following the European Council in March 2015, which tasked the High Representative to submit (in cooperation with the EU institutions and member states) an action plan on strategic communication to purposefully counter Russia's disinformation campaigns. The Task Force cooperates with the so-called myth-busting network of experts and NGOs in over 30 countries, reporting disinformation instances to the Task Force.[10]

The EU thus mostly sees its role in "creating synergies between all relevant instruments and fostering close cooperation between all relevant actors", capitalising on the existing (or at the time of the Framework's adoption still upcoming) tools, such as the European Agenda on Security, the EU Global Strategy for foreign and security policy and European Defence Action Plan, the EU Cybersecurity Strategy, the Energy Security Strategy, and the EU Maritime Security Strategy (EU 2016, p. 3). The Union's main institutional answer to the key task of enhancing awareness about hybrid threats by monitoring and evaluating the risks potentially targeting EU vulnerabilities is the EU Hybrid Fusion Cell, established within the EU Intelligence and Situation Centre (EU INTCEN) of the European External Action Service (EEAS). The Fusion Cell is tasked to monitor and analyse the "external aspects of hybrid threats, affecting the EU and its neighbourhood" (EU 2016, p. 4, Council of the European Union 2016), along with providing inputs to the security risk assessments carried out at the EU level. However, the Fusion Cell is not foreseen to offer policy recommendations or engage in strategic level research or capacity-building (via providing exercise or training) in countering hybrid threats. These functions are intended to be fulfilled by the recently established Centre of Excellence for Countering Hybrid Threats in Finland, which is open to both EU and NATO members (Finnish Government 2017). As per organisational reflex, the EU foresees a significant opportunity to reinvigorate the practical cooperation with NATO in their respective attempts to counter hybrid threats in the spheres of situational awareness, strategic communications, cybersecurity, and crisis prevention and response.[11] The new international Centre of Excellence is envisaged to be the pinnacle of this long-awaited cooperation. While designed to function outside regular EU and NATO structures as a multi-national network of sorts, this institution logically supplements the existing NATO Centres of Excellence on cyber defence in Tallinn, Estonia; strategic communications in Riga, Latvia, and energy security in Vilnius, Lithuania.[12]

NATO

"Hybrid warfare" has emerged as yet another "resilience test" (Stoltenberg 2015a) for the Alliance in its post-Cold War existential search for a new purpose and mission. Moreover, the hybrid insecurity predicament enables the allies to bring together the renewed focus on NATO's traditional mission (i.e. endorsing collective defence in order to counter the main geopolitical contestant of the North Atlantic Alliance in Europe) and the Alliance's post-Cold War out-of-area military expeditions. While "tak[ing] on two different forms of strategic challenges simultaneously" – that is, "the Russian hybrid warfare approach" and that of "other non-state actors like ISIS to the south" – remains NATO's "greatest challenge", the common idea behind these "hybrid strategies" endorses the relevance of "a comprehensive approach across the DIMEFIL spectrum" (i.e. diplomatic/political, information, military, economic, financial, intelligence, legal) for NATO (Breedlove 2015, p. xxv; cf. Bell 2012, pp. 225–226). The "beauty of the hybrid warfare concept" is accordingly seen to lie in its ability to "provide tools for a comparative strategic perspective of NATO's southern and eastern flanks, while allowing for a differentiated response" (Johnson 2015, p. 276). NATO's motto in the face of these twofold challenges is called to be "adopt, adapt, adept": the new strategies adopted to deal with the hybrid threats to NATO's East and South need to be accompanied by NATO's adaptation of "its structure and readiness to become adept at handling the new challenges it faces" (Calha 2015, p. 9).

Countering hybrid threats posed by Russia and the Islamic radicals threatening the territories, populations, interests, and values of the Alliance thus enables NATO to endorse its continuing relevance by constructing a strong narrative and maintaining its OS as the core security guarantor for its members (cf. Flockhart 2012, pp. 78–79). The softer, partnership-geared, or so-called "Jane" narrative of the early-post Cold War NATO is clearly giving way to a more familiar, hard security-focused "Tarzan" self-vision and public representation (see further Flockhart 2011). Calling the kettle black is the least of NATO's worries: Russia's use of "proxy soldiers, unmarked Special Forces, intimidation and propaganda, all to lay a thick fog of confusion; to obscure its true purpose in Ukraine; and to attempt deniability" is explicitly dissected in outlining NATO's emerging counter-strategy to hybrid engagements of the sort (Stoltenberg 2015a). Yet, just the traditional set of NATO's capabilities is clearly deemed to be insufficient in the face of, *inter alia*, "sophisticated disinformation and radicalization campaigns" (Stoltenberg 2015b), this more forceful and traditional antagonist-driven agenda reflects NATO's long-pursued comprehensive approach – that is, "a combination of military and non-military means to stabilize countries" (that others use to "destabilize") (Stoltenberg 2015a). "Hybrid" is accordingly coined as "the dark reflection" of NATO's comprehensive approach, and accordingly, early warning and situation awareness, good governance and the resilience of societies become equally essential parts of deterrence and defence against hybrid threats (Stoltenberg 2015a). This necessitates "renewed attention to strategic communications" and public outreach and education "to build up public awareness and resilience" and "strengthen the role of an informed civil society in every member state" (Calha 2015, p. 10).[13]

NATO declared its readiness to address the specific challenges posed by "hybrid warfare threats" in the Wales Summit Declaration of 5 September 2014 as a forceful response to the conflict in Ukraine. While NATO's traditional toolbox of collective defence is hardly perfectly geared for "insidious and ambiguous threats" (Johnson 2015, p. 270, Calha 2015,

p. 4), countering hybrid warfare emerges as a continuing relevance and resilience test for the Alliance. NATO's institutional responses to "hybrid threats" have been further detailed in its Readiness Action Plan, a roadmap for building capability packages, a comprehensive concept for creating an enhanced NATO response force, in a classified strategy for hybrid warfare and a cyber security action plan. Altogether, the ambiguity and gradient nature of hybrid tactics directly challenge the ontological underpinnings of NATO's core mission and strength as hybrid activities might "progress incrementally towards a threatening situation while remaining under NATO's Article 5 threshold" (Calha 2015, p. 4). The detection and definition of a threat hence becomes significantly less straightforward, pointing at the need to renegotiate the scope and substance of NATO's collective defence clause (i.e. Article 5 of the Washington Treaty) in light of the contemporary hybrid engagements.

Conclusion

This article has brought the notion of OS to bear on the thus far heavily policy-oriented hybrid warfare literature. As hybrid threats epitomise ontological insecurity, NATO and the EU's synergistic discourse and emerging practice on countering the hybrid menace emerges as an attempt at the institutionalisation of their organisational OS-seeking. Tackling the hybrid challenges of the day in apparent unison further provides NATO and the EU a silver lining of a tightened cooperation between the two organisations. Further research could map the complex interactions between the OS-seeking strategies of these distinct intergovernmental institutions and their member states/societies with regard to countering hybrid warfare. It would be interesting to investigate, for example, how the traditional lines of division within the European community along the more Russia-friendly and Russia-wary countries might tap into the institutional dynamics of hybrid threat management of the EU and NATO. Moreover, the newly established special sub-institutions to confront hybrid threats within the EU along with the organisationally unaffiliated Centre of Excellence could themselves develop their own identities, OS drives and placating routines, potentially generating organisational fragmentation and inter-agency tensions instead of bolstering the OS of the Union as a whole (cf. Steele 2017).

With regard to the ethical drawbacks of effective hybrid threat management, such an endeavour points at the problematic prospect of compromising the already fuzzy distinction between politics and war – as according to the hybrid warfare paradigm, all politics becomes reduced to the potential build-up phase for a full-blown confrontation. In that sense, hybrid warfare is close to the criteria of "minimal wars, which consist in *merely threatening the enemy with negotiations held in reserve*" (Clausewitz 1976, 604, emphasis in the original). The alleged "minimality" of such a way of warfare nonetheless has considerable potential to induce broad and deep securitisation of various public policy processes in the Western societies and their supranational organisations in question. Hybrid warfare and the emerging institutionalisation of its countering practices highlight the paradox of defending democratic security communities, as the efficacy of such defence might in fact be detrimental to some of the core organising principles of democracy.

An alternative approach would be to argue that hybrid warfare, and the countering practices it is generating, have simply brought the nature of the modern power out into the open. As Foucault maintains in his *Society Must Be Defended*, liberal "civil peace" must be understood as a secret form of war, for "war is the principle and motor of the exercise of

political power" in general (Foucault 2003, p. 18). Viewed from such a perspective, hybrid warfare and its emerging management practices by the EU and NATO enable us to see what politics is allegedly all about anyway – "the continuation of war by other means" (Foucault 2003, p. 15). For the EU and NATO, hybrid warfare embodies not just the unsettling of the politics/war distinction but raises the fundamental question about the practical distinguishability of their physical and ontological security in the first place.

Notes

1. Anthropologist Alexei Yurchak (2014) has invoked this expression to capture the Russian political technology of a military occupation staged as a non-occupation by anonymous troops without insignia.
2. E.g. "Hostile states pose 'fundamental threat'" (2016).
3. The IR literature on OS is steadily expanding. For a recent special issue on the concept, see *Cooperation and Conflict* (2017), edited by Catarina Kinnvall and Jennifer Mitzen, two of the key launchers of the notion in the discipline. For an authoritative book-length account, see Steele (2008).
4. See further Mitzen (2016) for the various types of "unthinkabilities" of war.
5. Yet, as Lupovici (2016) shows with his study of the idea and practices of deterrence, the ambiguity between peace and war is not invariably a source of ontological insecurity. Rather, as he argues, the "deterrer identity" has been a major base of OS for the United States and Israel throughout the Cold War and after.
6. I.e., defending "the EU, its Member States and citizens" from the "disinformation and misinformation campaigns and propaganda" (European Parliament 2016).
7. NATO's Strasbourg/Kehl Summit declaration (2009) maintains that

    it is increasingly important that the Alliance communicates in an appropriate, timely, accurate and responsive manner on its evolving roles, objectives and missions. Strategic communications are an integral part of our efforts to achieve the Alliance's political and military objectives.

8. See Sperling and Webber (2017) for a comprehensive take on NATO's (re)securitisation of Russia in connection with the Ukraine crisis.
9. Note that the EU is currently considering the applicability of its solidarity clause (Article 222 TFEU) "in case a wide-ranging and serious hybrid attack occurs" (European Commission 2017).
10. See http://collections.internetmemory.org/haeu/content/20160313172652/http://eeas.europa.eu/top_stories/2015/261115_stratcom-east_qanda_en.htm (accessed 5 April 2018). The EU Mythbusters are available on Twitter at https://twitter.com/EUvsDisinfo (accessed 5 April 2018).
11. See also http://www.nato.int/cps/en/natohq/opinions_131283.htm (accessed 5 April 2018).
12. Notably, Finland is not a member of NATO, so locating the new Centre there illustrates the purposeful bridge-building attempts of the two organisations in countering the hybrid menace together. The current members of the Centre are Finland, Sweden, the United Kingdom, Latvia, Lithuania, Poland, France, Germany, the United States, Estonia, Spain, Norway, the Netherlands, Italy, Czech Republic, and Denmark.
13. For NATO StratCom Centre of Excellence's definition of strategic communication-related activities and capabilities, see http://www.stratcomcoe.org/about-strategic-communications (accessed 5 April 2018). See also STRATCOMCOE@STRATCOMCOE.

Acknowledgements

European Conference on International Relations, Barcelona, September 2017. I am grateful to the two anonymous reviewers, Brent Steele, Alexandra Homolar, Ian Manners, Catarina Kinnvall, Jennifer Mitzen, Tuomas Forsberg, the respective workshop participants, Trine Flockhart, and Iver B. Neumann for their encouragement and genuinely helpful feedback. All remaining inconsistencies remain my responsibility.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Maria Mälksoo is Senior Lecturer in International Security at the Brussels School of International Studies, University of Kent. Her research interests lie at the intersection of critical security studies, memory and identity politics, international political sociology and critical IR theory. She is the author of *The Politics of Becoming European: A Study of Polish and Baltic Post-Cold War Security Imaginaries* (Routledge, 2010) and a co-author of *Remembering Katyn* (Polity, 2012). She has published on European security politics, liminality, memory wars, memory laws, transitional justice and foreign policy in Eastern Europe and Russia in the *International Studies Review, European Journal of International Relations, International Political Sociology, Security Dialogue, Review of International Studies, Contemporary Security Policy, Communist and Post-Communist Studies, Journal of Soviet and Post-Soviet Politics and Society, Cambridge Review of International Affairs*, and in various edited volumes.

ORCID

Maria Mälksoo http://orcid.org/0000-0002-7110-2050

References

Abulof, U., 2014. Deep securitization and Israel's "demographic demon". *International political sociology*, 8 (4), 396–415.

Barany, Z. and Rauchhaus, R., 2011. Explaining NATO's resilience: is international relations theory useful? *Contemporary security policy*, 32 (2), 286–307.

Barkawi, T., 2016. Decolonising war. *European journal of international security*, 1 (2), 199–214.

Bell, C., 2012. Hybrid warfare and its metaphors. *Humanity: an international journal of human rights, humanitarianism, and development*, 3 (2), 225–247.

Bourbeau, P. and Ryan, C., 2018. Resilience, resistance, infrapolitics and enmeshment. *European journal of international relations*, 24 (1), 221–239.

Breedlove, P.M., 2015. Foreword. *In*: G. Lasconjarias and J. A. Larsen, eds. *NATO's response to hybrid threats*. Rome: NATO Defense College, "NDC Forum Papers Series" Forum Paper 24, xxi–xxv.

Browning, P., 2002. *The changing nature of warfare: the development of land warfare from 1792 to 1945*. Cambridge: Cambridge University Press.

Browning, C. S, 2016. Ethics and ontological security. *In*: J. Nyman and A. Burke, eds. *Ethical security studies: a New research agenda*. London: Routledge, 160–173.

Browning, C. S. 2018. Brexit, Existential Anxiety and Ontological (In)Security. *European Security*, 27(3), 336–355.

Browning, C.S. and McDonald, M., 2013. The future of critical security studies: ethics and the politics of security. *European journal of international relations*, 19 (2), 235–255.

Browning, C.S. and Joenniemi, P., 2017. Ontological security, self-articulation and the securitization of identity. *Cooperation and conflict*, 52 (1), 31–47.

Calha, J.M. 2015. Hybrid warfare? NATO's new strategic challenge. *NATO Parliamentary Assembly Defence and Security Committee General Report*, 10 October, 166 DSC 15 E bis.

Clausewitz, C.v., 1976. *On war*. Princeton: Princeton University Press.

Cooper, R., 2004. *The breaking of nations: order and chaos in the twenty-first century*. Boston: Atlantic Monthly.

Council of the European Union. 2016. JOINT STAFF WORKING DOCUMENT EU operational protocol for countering hybrid threats "EU Playbook", SWD(2016) 227 final. Brussels, 7 July.

Creppell, I., 2011. The concept of normative threat. *International theory*, 3 (3), 450–487.

Croft, S. and Vaughan-Williams, N., 2017. Fit for purpose? Fitting ontological security studies "into" the discipline of international relations: towards a vernacular turn. *Cooperation and conflict*, 52 (1), 12–30.

Della Sala, V. 2018. Narrating Europe: The EU's Ontological Security Dilemma. *European Security*, 27 (3), 266–279.

Dingott Alkopher, T. 2018. Socio-Psychological Reactions in the EU to Immigration: From Regaining Ontological Security to Desecuritization. *European Security*, 27 (3), 314–335.

Ejdus, F., 2017. Critical situations, fundamental questions and ontological insecurity in world politics. *Journal of international relations and development*. https://doi.org/10.1057/s41268-017-0083-3.

European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, 2017. *Joint report to the European Parliament and the council on the implementation of the joint framework on countering hybrid threats – a European Union response*. Brussels, 19 July, JOIN (2017) 30 final. Available from: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2017:30:FIN [Accessed 5 April 2018].

European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 2016. Joint framework on countering hybrid threats: a European Union response. *Joint Communication to the European Parliament and the Council*. Brussels, April 6, JOIN(2016) 18 final.

European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 2017. *Joint communication to the European Parliament and the council: a strategic approach to resilience in the EU's external action*. Brussels, 7 June, JOIN(2017) 21 final.

European External Action Service, 2015. Food-for-thought paper "countering hybrid threats", EEAS (2015) 731, Political and Security Committee, 13 May. Available from: http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf [Accessed 5 April 2018].

European Parliament, 2016. EU strategic communication to counteract anti-EU propaganda by third parties. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)).

EU Mythbusters@EUvsDisinfo, *Twitter* (Accessed 5 April 2018).

Evans, M., 2003. From Kadesh to Kandahar: military theory and the future of war. *Naval war college review*, LVI (3), 132–150.

Ewald, F., 2002. The return of descartes's malicious demon: an outline of a philosophy of precaution. *In*: T. Baker and J. Simon, eds. *Embracing risk*. Chicago, IL: Chicago University Press, 273–302.

Finnish Government, 2017. European centre of excellence for countering hybrid threats established in Helsinki, 11 April. Press Release 159/2017. Available from: http://valtioneuvosto.fi/en/article/-/asset_publisher/10616/eurooppalainen-hybridiuhkien-osaamiskeskus-perustettiin-helsinkiin [Accessed 5 April 2018].

Flockhart, T., 2011. "Me Tarzan – you Jane": The EU and NATO and the reversal of roles. *Perspectives on European politics and society*, 12 (3), 263–282.

Flockhart, T., 2012. Towards a strong NATO narrative: from a "practice of talking" to a "practice of doing". *International politics*, 49 (1), 78–97.

Flockhart, T., 2016. The problem of change in constructivist theory: ontological security seeking and agent motivation. *Review of international studies*, 42 (5), 799–820.

Foucault, M., 2003. *"Society must be defended". Lectures at the Collège de France, 1975-76*. Trans. by David Macey. London: Penguin Books.

Franke, U., 2015. *War by non-military means: understanding Russian information warfare*. FOI-R--4065 —SE. Stockholm: Swedish Defence Research Agency.

Galeotti, M., 2015. Hybrid war as a war on governance. Interview by Octavian Manea. *Small Wars Journal*, 19 August.

Galeotti, M., 2016a. Hybrid, ambiguous, and non-linear? How new is Russia's "new way of war"? *Small wars & insurgencies*, 27 (2), 282–301.

Galeotti, M., 2016b. How to win Putin's information war. *The New York Times*, 15 December, A31.

Garton Ash, T., 2016. *Free speech: ten principles for a connected world*. London: Atlantic Books.

Gerasimov, V., 2013. The value of science in foresight: new challenges require rethinking on the forms and methods of warfare, presented at the Voroshilov Military Academy, reprinted in Tsennost' nauki v predvidenii. *Voenno-promyshlennyi kur'er*, 8 (476), 27 February – 5 March 2015, pp. 1–3. An English translation by Robert Coalson, Top Russian general lays Bare Putin's plan for Ukraine, *The Huffington Post*, 9 February 2014.

Giddens, A., 1990. *The consequences of modernity*. Stanford: Stanford University Press.

Giddens, A., 1991. *Modernity and self-identity: self and society in the late modern age*. Cambridge, UK: Polity.

Glenn, R.W., 2009. Thoughts on hybrid conflict. *Small Wars Journal*, 2 March.

Gray, C.S., 2007. *Another bloody century: future warfare*. London: Phoenix.

Greve, P., 2017. Ontological security, the struggle for recognition, and the maintenance of security communities. *Journal of international relations and development*. https://doi.org/10.1057/s41268-017-0108-y.

Henderson, E. and Singer, J., 2002. "New wars" and rumours of "new wars". *International interactions: empirical and theoretical research in international relations*, 28 (2), 165–190.

Hoffman, F.G., 2007. *Conflict in the 21st century: the rise of hybrid wars*. Arlington, VA: Potomac Institute for Policy Studies.

Hostile states pose "fundamental threat" to Europe, says MI6 chief, 2016. *The Guardian*, 8 December.

Huysmans, J., 1998. Security! What do you mean? From a concept to thick signifier. *European journal of international relations*, 4 (2), 226–255.

Ilves, T.H., 2016. Democracies face a fake new world. *The World Post*, 19 December.

Jacobs, A. and Lasconjarias, G., 2015. NATO's hybrid flanks: handling unconventional warfare in the south and the east. Rome: NATO Defense College, Research Paper no. 112 (April).

Johnson, D., 2015. Russia's approach to conflict – implications for NATO's deterrence and defence. *Research Paper no 111*, NATO Defense College, April.

Jonsson, O. and Seely, R., 2015. Russian full-spectrum conflict: an appraisal after Ukraine. *The journal of slavic military studies*, 28 (1), 1–22.

Juncos, A.E., 2017. Resilience as the new EU foreign policy paradigm: a pragmatist turn? *European security*, 26 (1), 1–18.

Kaldor, M., 1999. *New and old wars: organised violence in a global era*. Cambridge: Polity Press.

Kaldor, M., 2013. In defence of new wars. *Stability: international journal of security and development*, 2 (1), 1–16.

Kello, L., 2017. *The virtual weapon and international order*. New Haven: Yale University Press.

Kinnvall, C., 2004. Globalization and religious nationalism: self, identity, and the search for ontological security. *Political psychology*, 25 (5), 741–767.

Kinnvall, C. and Mitzen, J., eds., 2017. Ontological securities in world politics, *Cooperation and conflict*, 52 (1), Special Issue.

Kinnvall, C., Manners, I., and Mitzen, J. 2018. Introduction to 2018 special issue of European Security: "ontological (in)security in the European Union". *European Security*, 27 (3), 249–265.

Lupovici, A., 2016. *The power of deterrence: emotions, identity and American and Israeli wars of resolve*. Cambridge: Cambridge University Press.

Mälksoo, M., 2015. "Memory must be defended": beyond the politics of mnemonical security. *Security dialogue*, 46 (3), 221–237.

Mälksoo, M., 2016. From the ESS to the EU global strategy: external policy, internal purpose. *Contemporary security policy*, 37 (3), 374–388.

Manners, I., 2002. *European [security] Union: from existential threat to ontological security*. Copenhagen: Copenhagen Peace Research Institute.

McCuen, J., 2008. Hybrid Wars. *Military Review*, March–April.

Mitzen, J., 2006. Ontological security in world politics: state identity and the security dilemma. *European journal of international relations*, 12 (3), 341–370.

Mitzen, J., 2016. Security communities and the unthinkabilities of war. *Annual review of political science*, 19, 229–248.

Mitzen, J. and Schweller, R., 2011. Knowing the unknown unknowns: misplaced certainty and the onset of war. *Security studies*, 20 (1), 2–35.

Mitzen, J. 2018. Anxious Community: EU as (In)Security Community. *European Security*, 27 (3), 393–413.

Müller, J.-W., 2016. Protecting popular self-government from the people? New normative perspectives on militant democracy. *Annual review of political science*, 19, 249–265.

Münkler, H., 2005. *The new wars*. Cambridge: Polity Press.

Neocleous, M., 2007. Security, liberty and the myth of balance: towards a critique of security politics. *Contemporary political theory*, 6, 131–149.

Newman, E., 2004. The "new wars" debate: a historical perspective is needed. *Security dialogue*, 35 (2), 173–189.

Nietzsche, F., 2003. *Beyond good and evil*. Fairfield, IA: 1st World Library – Literary Society.

North Atlantic Council, 2009. Strasbourg/Kehl summit declaration, 4 April. Available from: http://www.nato.int/cps/bu/natohq/news_52837.htm?mode=pressrelease [Accessed 5 April 2018].

O'Connell, M.E., 2015. Myths of hybrid warfare. *Ethics and armed forces: controversies in military ethics & security policy*, 2. Available from: http://www.ethikundmilitaer.de/en/full-issues/20152-hybrid-warfare/oconnell-myths-of-hybrid-warfare/ [Accessed 5 April 2018].

Owens, P., 2012. Human security and the rise of the social. *Review of international studies*, 38 (3), 547–567.

Pawlak, P., 2015. Understanding hybrid threats. *EPRS At a Glance brief*, PE 564.355. Brussels, European Parliamentary Research Service.

Rathbun, B.C., 2007. Uncertain about uncertainty: understanding the multiple meanings of a crucial concept in international relations theory. *International studies quarterly*, 51, 533–557.

Reeves, S., 2016. The viability of the law of armed conflict in the age of hybrid warfare. *Lawfare*, 5 December. Available from: https://www.lawfareblog.com/viability-law-armed-conflict-age-hybrid-warfare [Accessed 5 April 2018].

Rossdale, C., 2015. Enclosing critique: the limits of ontological security. *International political sociology*, 9, 369–386.

Ruiz Palmer, D.A., 2015. Back to the future? Russia's hybrid warfare, revolutions in military affairs, and Cold War comparisons. *In*: G. Lasconjarias and J.A. Larsen, eds., *NATO's response to hybrid threats*. Rome: NATO Defense College, "NDC Forum Papers Series" Forum Paper 24, 49–71.

Rumelili, B., 2015. Ontological (in)security and peace anxieties: a framework for conflict resolution. *In*: B. Rumelili, ed. *Conflict resolution and ontological security: peace anxieties*. New York: Routledge, 10–29.

Rumelili, B. 2018. Breaking with Europe's Pasts: Memory, Reconciliation, and Ontological (In)security. *European Security*, 27 (3), 280–295.

Smith, R., 2005. *The utility of force: the art of war in the modern world*. London: Penguin Books.

Sperling, J. and Webber, M., 2017. NATO and the Ukraine crisis: collective securitisation. *European journal of international security*, 2 (1), 19–46.

Steele, B.J., 2008. *Ontological security in international relations: self-identity and the IR state*. London: Routledge.

Steele, B.J., 2017. Organizational processes and ontological (in)security: torture, the CIA and the United States. *Cooperation and conflict*, 52 (1), 69–89.

Stoltenberg, J., 2015a. Keynote speech by NATO secretary general Jens Stoltenberg at the opening of the NATO transformation seminar, 25 March. Available from: http://www.nato.int/cps/en/natohq/opinions_118435.htm?selectedLocale=en [Accessed 5 April 2018].

Stoltenberg, J., 2015b. Closing press conference by NATO secretary general Jens Stoltenberg following the meetings of NATO foreign ministers in Antalya, Turkey, 14 May. Available from: http://www.nato.int/cps/en/natohq/opinions_119432.htm [Accessed 5 April 2018].

Strachan, H. and Scheipers, S., 2011. *The changing character of war*. Oxford: Oxford University Press.

STRATCOMCOE@STRATCOMCOE, *Twitter*. Available from: https://twitter.com/STRATCOMCOE [Accessed 5 April 2018].

Subotic, J. 2018. Political Memory, Ontological Security, and Holocaust Remembrance in Post-Communist Europe. *European Security*, 27 (3), 296–313.

Tenenbaum, E., 2015. Le piège de la guerre hybride. *IFRI Focus stratégiqu*e n° 63 (Octobre). Paris: IFRI.

Vieira, M.A., 2016. Understanding resilience in international relations: the non-aligned movement and ontological security. *International studies review*, 18 (2), 290–311.

Wagner, W. and Anholt, R., 2016. Resilience as the EU global strategy's new leitmotif: pragmatic, problematic or promising? *Contemporary security policy*, 37 (3), 414–430.

Waldron, J., 2003. Security and liberty: the image of balance. *Journal of political philosophy*, 11 (2), 191–210.

Walt, S., 1991. The renaissance of security studies. *International studies quarterly*, 35 (2), 211–239.

Winter, Y., 2011. The asymmetric war discourse and its moral economies: a critique. *International theory*, 3 (3), 488–514.

Yurchak, A., 2014. Little green men: Russia, Ukraine and post-Soviet sovereignty. Anthropoliteia, 31 March. Available from: https://anthropoliteia.net/2014/03/31/little-green-men-russia-ukraine-and-post-soviet-sovereignty/ [Accessed 7 July 2018].