Cullen, Patrick. "A perspective on EU hybrid threat early warning efforts." *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. By Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm . London: I.B. Tauris, 2021. 46–57. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781788317795.0009>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 14:17 UTC.

Copyright © Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm 2021.
Released under a CC BY-NC-ND licence (<https://creativecommons.org/licenses/by-nc-nd/3.0/>).
You may share this work for non-commercial purposes only, provided you give attribution to the copyright holder and the publisher, and provide a link to the Creative Commons licence.

A perspective on EU hybrid threat early warning efforts

Patrick Cullen

The EU's introduction to hybrid threats

The European understanding and appropriation of the terms 'hybrid threats' and 'hybrid warfare' cannot be understood without reference to the Russian annexation of Crimea in 2014. This aggression in Ukraine – combined with the view that Russia had employed a novel (if not precisely new) style of warfighting – marked a sea-change in the European perceptions of their security environment. NATO applied the moniker hybrid warfare to this event and immediately organized a 'hybrid warfare' deterrence posture built around enhancing its ability to deploy a rapid conventional military response to reassure its eastern members within the Alliance.¹ Others, however, had observed that NATO was ill-equipped to respond to some of the most troubling attributes of what was now being referred to as hybrid warfare; the use of ambiguity, non-attributability, coordinated use of non-military tools (e.g. cyber, economic, financial, information), and the deliberate manipulation of detection, political decision-making and military response thresholds capable of complicating NATO's ability to invoke collective self-defence. Not for the first time,² NATO began discussing a need for greater security cooperation between NATO and the European government and civil society actors to address the threats implied by these developments; hybrid threats that could be non-military in nature, that could manifest and cause damage to one's society prior to any military action by the aggressor, and that otherwise fell below or outside the remit of NATO defence responsibilities.³

By early 2015 the view that hybrid warfare had exposed a security gap below the threshold of war that could not be filled by NATO and thus required other governmental bodies such as the EU to directly engage in countering this threat was gaining traction. A new European security discourse on 'the changed security environment, often described as hybrid warfare'⁴ was being adopted by EU leadership, and it had begun tasking various EU organs like the European Defense Agency and the European External Action Service (EEAS) with developing plans for countering hybrid threats. By March 2015 the EEAS had launched the East StratCom Task Force to counter Russian disinformation campaigns. By May it released a 'Food for thought

paper: Countering Hybrid Threats' that explicitly labelled both 'Russia's aggression in Ukraine' and the 'advances and morphing of Daësh', respectively, as eastern and southern hybrid threats.⁵ This document provided a series of proposals that would heavily influence the EU's response to hybrid threats and also informed the EU's collaboration with NATO in the 2016 and 2018 EU-NATO Joint Declarations.

These Joint Declarations essentially institutionalized the vision that each organization could – and should – collaborate more closely in order to close the previously mentioned security gap that allowed adversaries to inflict damage on societies within the EU and its partner nations by deploying hybrid threats in the grey zone between peace and war.⁶ Within this context, the EU's 'Joint Framework on countering hybrid threats: a European Union response'⁷ and subsequent EU documents on countering hybrid threats outlined twenty-two actions to be undertaken. These efforts focused on early warning and situational awareness, strategic communication, crisis response and resilience building.⁸

Understanding how the EU conceptualized hybrid threats is critical for understanding how and why the EU was tasked with these new responsibilities (and opportunities) to enhance its role in European security-making. The remainder of this chapter is organized as follows. The next section will briefly elaborate EU descriptions of hybrid threats. Thereafter, the focus will move to how the EU has approached early warning/detection of hybrid threats. Specifically, it will address how this security problem created a push for an enhanced EU-wide situational awareness mechanism that was embedded in the newly created EEAS Hybrid Fusion Cell. The chapter concludes with a discussion of joint EU-NATO efforts at enhanced hybrid threat situational awareness.

Describing rather than defining hybrid threats

One can readily find early references to both hybrid *warfare* and hybrid *threats* within various EU speeches, papers and webpages. In the past, the two terms have even been used interchangeably within the same document. For instance, an EEAS paper from 2015 with a section entitled 'defining hybrid threats' began by noting that 'hybrid warfare can be more easily characterized than defined'.⁹ Although these terminological hurdles have not yet disappeared, an early political (rather than analytical) consensus has emerged within the EU that it should focus on the less politically charged language of countering of hybrid *threats* while leaving the business of countering hybrid *warfare* to its member states and NATO.¹⁰ In practice, however, the hybrid threat/warfare distinction was left largely unexplored by the EU between 2015 and 2018, although this distinction has been made in a forthcoming document on hybrid threats sponsored by the European Commission.¹¹ The pragmatic and policy-oriented focus of the EU's approach to its counter-hybrid efforts also explains why the EU has chosen to *describe* rather than *define* hybrid threats. If a precise definition proved divisive or elusive, an adequate description of hybrid threats could facilitate the rapid development of an EU counter-hybrid-threats policy. This focus on political action took precedent

over entering a heated definitional debate that was already almost a decade old by 2015 (and that showed no indication of slowing down). Academic and professional military criticism that argued the terms 'hybrid warfare and threats' were too vague and imprecise were considered less important in this context.¹² As a result, the 2016 EU Joint Framework *described* hybrid threats concept as follows:

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 (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. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalize, recruit and direct proxy actors can be vehicles for hybrid threats.¹³

And this approach seems to be working for the EU. As one EU research centre noted:

Quite simply: the term 'hybrid threats' is already being used and understood by EU officials and government representatives to capture a range of non-conventional security challenges. Whether in healthcare and/or transport, the 'hybrid' label is encouraging staff in various EU bodies to give more consideration to the security aspects of their respective portfolios than perhaps has been the case in the past.¹⁴

The next section explores this development in the context of EU hybrid threat detection and early warning.

An EU approach to early warning: Leveraging non-military civilian expertise

The very thing that makes the EU vulnerable to hybrid threats – namely, its position as a governing body with responsibilities over a wide spectrum of civil functions and critical infrastructure across different sectors of the economy and society – also *in principle* provides it with the institutionalized professional expertise that can usefully be applied to counter hybrid threats targeting these same civilian spaces. Properly organized and coordinated into a security mechanism, sector-level expertise – in areas such as transport, health, financial, maritime, energy – held within various civil EU agencies can be exploited in hybrid threat early warning efforts. Importantly, this civilian expertise can be used to supplement the more military-centric early warning and detection efforts of NATO that does not have the same in-house skillset or political mandate to conduct these types of hybrid threat situational awareness measures in civil society.¹⁵ Beyond this civilian skillset, the multinational character of the EU has also been highlighted as

a reason why it is natural for it to become a security provider when confronting hybrid threats that have complex ‘comprehensive’ and transnational characteristics.¹⁶

In aspirational terms, and as shown later, the EU is slowly re-interpreting a role for itself in leveraging its broad non-military skillset as a complement to parallel military (e.g. EU member state military/intelligence and NATO) counter-hybrid early warning efforts. It is doing this by using various EU departments and executive agencies to play a role in anticipating (or even identifying) activities or trends with their respective areas of expertise that may be related to hybrid threats that deliberately attempt to use non-military tools and other ambiguous means to damage or otherwise negatively influence targets in the EU. The EEAS has discussed the possibility of this EU-NATO synergy at the strategic level, explaining that ‘(g)iven the fact that both organizations bring different competencies to bear, there is a rare chance to collaborate on building complimentary and mutually supportive strategies while retaining the autonomy of actions in both organisations.’¹⁷ Thus, even though the EU continues to emphasize that member states have ‘the primary responsibility’ for countering hybrid threats as a matter of national defence – not least because ‘most national vulnerabilities are country-specific’¹⁸ – the EU clearly sees an important and even necessary role for itself in countering hybrid threats that includes hybrid threat identification and early warning. This is no small task. As Fiott and Parks note,

the major test is to be able to prove with some degree of certainty that the combination of threats facing the EU at any given moment amounts to a hybrid campaign involving an external actor. In other words, when is a disruption to the EU’s food supply simply a case of negligence or criminal behaviour and when does it become part of a hybrid campaign.¹⁹

Some of the earliest publicly available work on the EU approach to building a system of hybrid threat early warning can be found in the EEAS 2015 Food-for-Thought paper.²⁰ In a section entitled ‘Improve Awareness’, the paper outlined and recommended a straightforward approach to hybrid threat early warning that can be summed up in three steps:

- 1) Conduct vulnerability assessments to recognize and understand weaknesses to hybrid threats;
- 2) Acquire and maintain a sufficient level of situational awareness capable of detecting subtle (e.g. nontraditional, covert or ambiguous) hybrid threats;
- 3) Create an analytical cell within the EU tasked with developing methodologies for monitoring this situational awareness apparatus to ‘recognize subtle changes to the threat landscape, which later may turn out to be elements of an (hybrid) adversary’s larger campaign.’²¹

Vulnerability assessments

Despite the difficulties involved (addressed later), progress has been made by the EU in each of these three areas. Hybrid threat vulnerability assessments have been pursued

through a mechanism called ‘Friends of the Presidency Group on hybrid threats (FoP)’. The FoP launched a hybrid risk survey programme tasked with coordinating surveys to identify key vulnerabilities potentially affecting national and pan-European structures and networks and began with a survey in Europe’s ‘neighbourhood regions’.²² This work has been extended from 2018 to 2020 to coordinate ‘surveys and key vulnerability assessments’ of hybrid threats across the EU.²³ The FoP survey relies on national self-reporting, a method that acknowledges that the actual process of vulnerability mapping is itself a highly sensitive process that is best done at the national level. Rather than trying to conduct this work directly, the EU has positioned itself as a resource to assist individual nations with this work, and to act as a conduit to share information from vulnerability assessments provided by states related to hybrid threats. The FoP has also attempted to collect ‘specific hybrid related indicators’ from EU member and partner states that could potentially be shared across the EU to enhance readiness and early warning.²⁴

In practice, this task of collecting vulnerability assessments and indicators has proven difficult, and other EU organizations have also encountered difficulties in this area. For instance, the EU border security organization Frontex was given authority in 2016 to carry out Schengen border threat assessments. Yet its efforts to create a comprehensive picture of Schengen border vulnerabilities were impaired by states’ unwillingness to share such information with EU agencies due to concerns over both security leaks of sensitive information, or political embarrassment or censure due to admission of poor national border security practices.²⁵ Despite progress in EU hybrid threat vulnerability assessment efforts, this problem of states only sharing the most minimally useful information has also negatively impacted FoP efforts.

Hybrid threat situational awareness: Leveraging existing mechanisms

The second key aspect of the EU approach to building hybrid threat situational awareness leverages builds upon institutionalized EU security practices and frameworks that are already in place. The logic underpinning this approach was simple: save time and money while minimizing the impact on EU agencies by embedding hybrid threat early warning tasks and responsibilities into pre-existing strategies, agencies and institutions. This approach was used across the board, and impacted the EU Cybersecurity Strategy, the Energy Security Strategy and the European Union Maritime Security Strategy, among others. The Maritime Security Strategy, for example, was reformulated to enable ‘the EU and its member states to tackle maritime security challenges, including countering hybrid threats, through cross-sectoral cooperation between civilian and military actors’.²⁶ The perceived value-added of the counter-hybrid threat efforts – and a prerequisite for its effectiveness – has been to break down legal, institutional and cultural barriers to information sharing and to create a ‘holistic approach’ that develops ‘synergies’ with close cooperation between relevant actors, institutions, strategies and sectors.²⁷ It was this development of closer coordination and communication between

EU bodies that ‘are exposed to or have sight of hybrid threats and indicators’ that has been viewed as crucial for building a warning model for hybrid threats. And this is at the core of EU attempts at contributing to hybrid threat situational awareness.²⁸

Much of the emphasis on hybrid threat early warning and situational awareness is being operationalized and built into pre-existing EU efforts at critical infrastructure protection. This is driven by an understanding that ‘an unconventional attack by perpetrators of hybrid threats on any “soft target” could lead to serious economic or societal disruption.’²⁹ One example of a pre-existing effort is the European Programme for Critical Infrastructure Protection (EPCIP). This program uses the type of all-hazard and cross-sectoral approach – including a vulnerability analysis that looks for critical interdependencies – that is well-suited to deal with hybrid threats, and as a result to EPCIP is being re-evaluated as a tool to address cross-sectoral hybrid threats.³⁰ The fact that many of these EU responses to hybrid threats had already existed (or were in the legislative pipeline) prior to and independently of the EU’s focus on combatting hybrid threats³¹ has also led to some questions regarding what new organizational initiatives, if any, the EU has undertaken to deal with hybrid threat early warning.

EU Hybrid Fusion Cell

The answer to the earlier question of what, if any, new EU organizational initiatives have been dedicated to hybrid threat warning intelligence can be seen in the implementation of the third EEAS recommendation: establishing an analysis unit focusing on hybrid threat situational awareness. The creation of an EU counter-hybrid threat warning intelligence system was born in the shape of the EU Hybrid Fusion Cell that was established in 2016. Located within the EU Intelligence and Situation Centre (EU INTCEN) of the EEAS, it was originally designed to provide ‘all source analysis’³² on hybrid threats and is the designated focal point for intelligence related to potential hybrid threats.³³ Following the pattern of embedding counter-hybrid threat early warning efforts into pre-existing systems already in place within various EU agencies, setting up a hybrid fusion cell located within a pre-existing EU situation centre was described by EEAS as a ‘quick win’ that could be established without creating a strain on EU resources.

The fundamental purpose of the Cell was based on a perceived need for a fusion of pre-existing knowledge and inefficiently siloed patches of situational awareness into a single pan-EU whole. After an internal review process of EU capacity for early warning/situational awareness, EEAS originally argued that there already existed ‘a good number of indicators and warnings from across the broad range of EU competencies that could support a very effective form of early warning.’³⁴ What was needed, from their perspective, was the formation of an effective clearinghouse, or ‘marketplace’ where member states and various other EU bodies and third party institutions, including NATO and the Centre of Excellence for Countering Hybrid Threats, could collaborate and share relevant information and where appropriate, intelligence.³⁵

It was thus set up with the aspiration to act as a point of entry for member states and other partners who had experienced hybrid threats in order to shares best

practices, warning indicators and lessons learned; raise awareness of vulnerabilities to hybrid threats and promote education related to hybrid threats and early warning. From the outset, EU Member States were encouraged to establish National Contact Points tied to the EU Hybrid Fusion Cell to facilitate outreach and information sharing. This process was repeated internally within the EU itself, with various EU personnel designated as Internal Points of Contact to represent their EU service agency on all matters related to hybrid threats.³⁶ In this way, the EU Hybrid Fusion Cell was designed to look both internally and externally for hybrid threats. It would receive and analyse information on foreign hybrid threats taken from foreign EU Delegations located in non-EU countries, as well as liaising with EU Commission services to collect and analyse cross-sector information on hybrid threats from an intra-EU perspective.

The EU Hybrid Fusion Cell has thus been designed as the primary hub in a wide multi-actor information-sharing network of counter-hybrid threat nodes (i.e. actors and activities) that span across (and into the organs and capillaries) the EU organization, as well as into partner nations and partner institutions. This role has been both an aspiration and a political responsibility. In aspirational terms, once all this information had been collected into a unified picture, the EU Hybrid Fusion Cell was foreseen to be able to provide hybrid threat warning intelligence to EU leadership. In terms of political responsibility, the director of INTCEN, as the senior Fusion Cell official, had been tasked with rapidly analysing incidents possibly related to a hybrid threat to inform EU strategic decision-making processes, and other policy and operational levels.³⁷ For instance, when the Fusion Cell's analysis indicates the possible existence of a hybrid threat against either a member state or a partner organization or nation, the director of INTCEN is responsible for using established rapid-reaction protocols to first inform relevant parties at the operational level to urgently respond to the potential threat.³⁸

Yet when it comes to a discussion of the methodologies and techniques that the EU Hybrid Fusion Cell is using to identify possible hybrid threats, public details have been (perhaps understandably) limited. One key effort that has been highlighted is the need to train EU staff – including deployed EU staff in delegations, operations and missions – to be able to ‘recognize early signs of hybrid threats’.³⁹ This is a crucial component in any hybrid threat situational awareness effort, because the Fusion Cell will rely on the ability of EU personnel to identify early indications and weak signals of possible hybrid threats affecting their area of responsibility, and then feeding this information to the Fusion Cell for analysis. Arguably, one paradox relating to the EU's recognition that it must train its personnel to ‘see’ hybrid threats is the EEAS' argument (discussed earlier) that many EU agencies already have the necessary indicators and early warning systems in place and that the only thing required for the Fusion Cell is to act as a clearing house to sync all of them up into an EU-wide, coherent whole. If this observation is accurate, then very little actual training would be required, and the solution for an effective hybrid warfare situational awareness could instead be effectively resolved with a legal-organizational solution. In other words, training analysts in new methodologies designed to detect ambiguous hybrid threats would be irrelevant, since each EU agency already has the early warning indicators needed to

detect them. This begs the question as to whether these indicators are standardized in a way that allows for meaningful comparison, and whether they are flexible or creative enough to identify hybrid threats that may be intentionally designed to maximize ambiguity.

However, in at least one area, the EU (i.e. the EEAS specifically) has explained a way in which the EU Hybrid Fusion Cell would be uniquely positioned to identify hybrid threats before any other EU warning system would be able to do so. That is, by using its fused situational awareness to connect the dots into a broader pattern recognition intelligence product, effectively linking a series of low threshold, ambiguous incidents across multiple EU agencies/sectors and thus identifying a (possible) wider hybrid threat campaign. This cross-agency work is facilitated in part by a monthly roundtable meeting at the Hybrid Fusion Cell with representatives from participating EC Directorate Generals. By signalling both a need to achieve this level of situational awareness with concrete plans for the Fusion Cell to work towards it, the Cell's work already transcends a simple collection and fusion of early warning indicators from across the EU. Other discussions of methods related to early warning against hybrid threats within the EU have been rather sparse and piecemeal but give some idea about the kinds of intelligence products they foresee the Fusion Cell providing. For instance, the EEAS has written about using various forms of structured analytic techniques – albeit in very broad language – such as mentioning that ‘this virtual fusion cell could include elements such as strategic foresight and early warning and be supported by scientific research’,⁴⁰ and that ‘the cell could catalyze all indicators . . . and then analyze them against a possible hybrid attack scenario both in EU MS and third countries’.⁴¹

Other warning intelligence efforts undertaken by the EU that fall outside of the efforts of the Hybrid Fusion Cell – but that are clearly central to EU hybrid threat early warning – include work in the strategic communication space. In one example, EEAS STRATCOM EAST does a weekly analysis of Russian disinformation campaigns with one of its key goals as building an improved EU capacity to forecast disinformation activities by external actors.⁴²

EU-NATO counter-hybrid early warning: Parallel and coordinated, not joint

NATO secretary Jens Stoltenberg has described the type of pattern recognition required for hybrid threat early warning in order to strip it of its ambiguity when he stated the following:

To be prepared, we must be able to see and analyze correctly what is happening; to see the patterns behind events which appear isolated and random; and quickly identify who is behind and why. So therefore, we need to sharpen our early warning and improve our situation awareness. This is about intelligence, expert knowledge and analytical capacity. So we know when an attack is an attack.⁴³

This emphasis on being able to 'see the patterns behind events which appear isolated and random' is precisely one of the stated goals of the EU Hybrid Fusion Cell.

However, despite the EU-NATO Joint Declaration's calls for closer cooperation, political directives have placed limitations on the degree to which the EU Hybrid Fusion Cell can work with its NATO counterpart, the NATO Hybrid Analysis Branch. The two organizations are not allowed to share intelligence. Instead, they can conduct 'parallel and coordinated assessments' involving discussion of open source materials, the coordination of requests for information (from member state intelligence organizations) and regular meetings.⁴⁴

In this political context, much of the EU-NATO collaboration in countering hybrid threats mirrors the EU's internal process of building on previously existing security programmes. This can be seen in the way EU-NATO collaboration in the realm of cyber defence is being conceptualized and packaged as a counter-hybrid effort. In practical terms senior staff to staff meetings between European Union Military Staff, the EDA and NATO C3 staff held in 2015 helped catalyse regular cooperation at the working level. Cross-briefings on cyber defence took place on a regular basis, and this in turn helped institutionalize collaboration in cyber defence capabilities development. NATO was accepted as an official observer in the EDA cyber ranges project, and NATO reciprocated by inviting the EDA to participate in NATO cyber education, training and exercises.⁴⁵ EU-NATO collaboration in early warning and detection in the cyber domain was specifically addressed in 2016 when the EU and NATO completed a technical arrangement between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team – European Union (CERT-EU). Reportedly, this technical information sharing 'will be achieved, for instance, through the sharing of routine information exchange products, (e.g. non-public indicators of compromise, situational awareness, reports) as well as visits to facilities and laboratories'.⁴⁶ In the context of formal restrictions on how the EU and NATO can share intelligence, collaboration in countering and detecting hybrid threats will likely be driven by embedding the hybrid problem into already ongoing programmes, as well as by grassroots person-to-person and bottom-up efforts to find practical ways to enhance cooperation between these organizations.

Conclusion

Both the EU's engagement with hybrid threats and its emphasis on early warning and detection have been heavily influenced by Russia's invasion of Ukraine. Not only did this aggression fundamentally realign EU perceptions of Russian intentions as a security threat, but the nature of Russian tactics in Ukraine also revealed it was willing and able to experiment with ambiguous methods of political coercion that threatened Europe in novel ways below the level of actual war (and a NATO Article 5 collective self-defence response). This recognition within the EU and NATO – and their member states – created the impetus for the EU to focus on countering hybrid threats in a newly recognized security gap below the threshold of war that NATO is ill-equipped to respond to.

A significant portion of this EU has focused on identifying hybrid threats in their early stages, and the EU has made considerable progress in these efforts. In the realm of early warning and detection, the EEAS' recommendations made in 2015 focusing on vulnerability assessments, the development of an EU-wide cross-sector situational awareness concept, and the creation of a dedicated fusion cell designed to monitor this joined-up threat landscape have all been implemented. However, these successes have not come without challenges. Creating new information-sharing practices across organizations and cultures is difficult under the best circumstances, and is especially difficult in security matters. With the EEAS and the Hybrid Fusion Cell heavily reliant on the active cooperation of member state intelligence agencies and EU departments for their information, early aspirations for the Cell to be able to provide its clients with actionable intelligence at the tactical or operational level have been replaced with a focus on providing long-term intelligence and trend analysis at the strategic level. Despite some of the practical and political limitations imposed on these EU early warning, the efforts by the Hybrid Fusion Cell represent a significant step in the right direction towards filling the security gap below NATO's Article 5 that hybrid threats seek to exploit.

Notes

- 1 Atlantic Council, 'Breedlove: NATO Have Begun Shaping Rapid Response Force', *Commanders Series*, 17 September 2014.
- 2 Michael Aaronson, Sverre Deisen, Yves de Kermabom, Mary Beth Long and Michael Miklaucic, 'NATO: Countering the Hybrid Threat', *PRISM* 2, no. 4 (2011): 111–24.
- 3 Peter Pindjak, 'Deterring Hybrid Warfare: A Chance for NATO and the EU to Work Together?' *NATO Review*, 18 November 2014.
- 4 European Defense Agency, 'Hybrid Warfare', 16 July 2015. <https://www.eda.europa.eu/what-we-do/activities/activities-search/hybrid-warfare>.
- 5 EEAS, 'Food for Thought Paper "Countering Hybrid Threats"', 13 May 2015. <https://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf>, 2.
- 6 Daniel Fiott and Roderick Parkes, 'Protecting Europe: The EU's Response to Hybrid Threats', *EUISS Chailiot Paper* 151, April 2019, 6.
- 7 European Commission, 'Joint Framework for Countering Hybrid Threats', 6 April 2016.
- 8 Hanna Smith, 'Countering Hybrid Threats', in *The EU and NATO: The Essential Partners*, eds Gustav Lindstrom and Thierry Tardy (EUISS: Paris, 2019), 17.
- 9 EEAS, 'Food for Thought Paper "Countering Hybrid Threats"', 2.
- 10 Interviews with EU officials working on hybrid threats have stated to the author that the European Commission has 'insisted' on the term threat rather than warfare.
- 11 This forthcoming publication is a joint product of the EC's Joint Research Centre and the European and the European Centre of Excellence for Countering Hybrid Threats. The author contributed to its development.
- 12 The Counter Hybrid Warfare project of MCDC, another multinational armed forces initiative, had also adopted this position of describing rather than defining hybrid warfare by 2015. This position has since been replicated by the European Centre of

- Excellence for Countering Hybrid Threats and other organizations, including NATO Strategic Communications Centre of Excellence.
- 13 European Commission, 'Joint Framework for Countering Hybrid Threats', 2.
 - 14 Fiott and Parkes, 'Protecting Europe: The EU's Response to Hybrid Threats', 8.
 - 15 Personnel from numerous EC Directorate Generals participating in the March 2016 EDA Hybrid Threats Table Top Exercise made this point during the exercise. Author participation, 11 March 2016, Brussels.
 - 16 Margriet Drent, Rob Hendriks and Dick Zandee, 'New Threats, New EU and NATO Responses', *Clingendael Report*, July 2015, 38–43.
 - 17 EEAS, 'Food for Thought Paper "Countering Hybrid Threats"', 5.
 - 18 European Commission Fact Sheet, 'FAQ: Joint Framework on Countering Hybrid Threats', 6 April 2016, Brussels, 1.
 - 19 Fiott and Parkes, 'Protecting Europe: The EU's Response to Hybrid Threats', 9.
 - 20 EEAS, 'Food for Thought Paper "Countering Hybrid Threats"'.
 - 21 Parentheses added. EEAS, 'Food for Thought Paper "Countering Hybrid Threats"', 4.
 - 22 Author discussion with EEAS official, also see European Commission, 'Joint Framework for Countering Hybrid Threats', 15.
 - 23 Fiott and Parkes, 'Protecting Europe: The EU's Response to Hybrid Threats', 32.
 - 24 European Commission, 'Joint Framework for Countering Hybrid Threats', 3.
 - 25 Fiott and Parkes, 'Protecting Europe: The EU's Response to Hybrid Threats', 12.
 - 26 Fiott and Parkes, 'Protecting Europe: The EU's Response to Hybrid Threats', 7.
 - 27 Fiott and Parkes, 'Protecting Europe: The EU's Response to Hybrid Threats', 3.
 - 28 EEAS, 'Food for Thought Paper "Countering Hybrid Threats"', 4.
 - 29 European Commission, 'Joint Framework for Countering Hybrid Threats', 6.
 - 30 European Commission, 'Joint Framework for Countering Hybrid Threats'.
 - 31 Jan Jakub uzieblo, 'United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats', *EU Diplomacy Paper*, College of Europe, Brugge, May 2017, 22.
 - 32 European Commission, 'Security and Defense: Significant Progress to Enhance Europe's Resilience against Hybrid Threats—More Work Ahead', Press Release, Brussels, 19 July 2017. https://ec.europa.eu/commission/presscorner/detail/en/IP_17_2064.
 - 33 European Commission, 'EU Playbook: Operational Protocol for Countering Hybrid Threats', Brussels, 5 July 2016, 5.
 - 34 EEAS, 'Food for Thought Paper "Countering Hybrid Threats"', 4.
 - 35 EEAS, 'Food for Thought Paper "Countering Hybrid Threats"', 4.
 - 36 European Commission, 'EU Playbook: Operational Protocol for Countering Hybrid Threats', 5.
 - 37 European Commission, 'EU Playbook: Operational Protocol for Countering Hybrid Threats'.
 - 38 European Commission, 'EU Playbook: Operational Protocol for Countering Hybrid Threats', 9.
 - 39 European Commission, 'EU Playbook: Operational Protocol for Countering Hybrid Threats'.
 - 40 EEAS, 'Food for Thought Paper "Countering Hybrid Threats"', 4.
 - 41 EEAS, 'Food for Thought Paper "Countering Hybrid Threats"'.
 - 42 EEAS, 'Questions and Answers about the East Stratcom Task Force', 26 November 2015. http://collections.internetmemory.org/haeu/content/20160313172652/http://eeas.europa.eu/top_stories/2015/261115_stratcom-east_qanda_en.htm.

- 43 Jens Stoltenberg, keynote speech, NATO Transformation Seminar, 25 March 2015.
https://www.nato.int/cps/ic/natohq/opinions_118435.htm.
- 44 Interviews with EC and NATO personnel, 27 February 2018.
- 45 Patryk Pawlak, 'Countering Hybrid Threats: EU-NATO Cooperation', *European Parliamentary Research Service*, March 2017, 10.
- 46 Pawlak, 'Countering Hybrid Threats: EU-NATO Cooperation'.