Article

Wilfried Martens Centre for European Studies

European View
2021, Vol. 20(1) 23–33

DOI: 10.1177/17816858211004648
journals.sagepub.com/home/euv
SAGE

Strengthening the EU's resilience to hybrid threats

Sandra Kalniete and Tomass Pildegovičs

Abstract

Against the backdrop of the deterioration of EU–Russia relations in recent years, there has been a shift in the awareness of hybrid threats all across the Union. At the same time, there is evidence of a growing political will to strengthen resilience to these threats. While hostile foreign actors have long deployed hybrid methods to target Europe, Russia's intervention in Ukraine in 2014, interference in the 2016 US presidential election, and repeated cyber-attacks and disinformation campaigns aimed at EU member states have marked a turning point, exposing Western countries' unpreparedness and vulnerability to these threats. This article analyses the EU's resilience to hybrid warfare from institutional, regulatory and societal perspectives, with a particular focus on the information space. By drawing on case studies from member states historically at the forefront of resisting and countering Russian-backed disinformation campaigns, this article outlines the case for a whole-of-society approach to countering hybrid threats and underscores the need for EU leadership in a standard-setting capacity.

Keywords

EU, Russia, Security, Hybrid threats, Resilience

Introduction

In recent years, the EU and its like-minded partners around the world have woken up to the persistent and acute dangers posed by hybrid threats. While hostile state and non-state actors have long deployed hybrid methods to target the EU, Russia's hybrid warfare in Ukraine in 2014, along with its interference in the 2016 US presidential election, marked a turning point, exposing Western countries' unpreparedness and vulnerability to these threats (Renz 2016). Russia's brazen interference in democratic processes explicitly demonstrated that the EU and its member states lacked response mechanisms to engage with

Corresponding author:
S. Kalniete, European Parliament, Rue Wiertz 60, Bruxelles, B-1047, Belgium.
Email: sandra.kalniete@europarl.europa.eu

emergent threats that did not constitute direct aggression but rather sought to undermine their political decision-making, cohesion and capacity for collective action (Marovic 2019). In recent years, we have witnessed numerous other instances of Russian foreign interference in the domestic affairs of EU countries, including meddling in the 2016 Brexit referendum (Sabbagh et al. 2020); financing far-right political parties in France, Hungary and Germany (Rettman 2017); spreading disinformation regarding the downing of flight MH17 (Kent 2020); and conducting targeted assassination attempts in the UK (Corera 2020) and Germany (*Deutsche Welle* 2020). At present, Europe faces a barrage of Russian disinformation regarding the COVID-19 crisis, which is cynically endangering human lives by sowing doubt about the safety of approved vaccines and the credibility of the imposed restrictions (EEAS 2020). While foreign interference or disinformation is a phenomenon by no means unique to Russia, with other state and non-state actors deploying such methods to target the EU for political or commercial reasons, this article will consider the issue of hybrid threats within the broader geopolitical context of EU–Russia relations.

The aim of this article is to examine the EU's resilience to hybrid warfare from institutional, regulatory and societal perspectives, with a particular focus on the information space. Recognising that a wide range of activities can be subsumed under the umbrella term of 'hybrid threats', this article makes the methodological choice to focus on disinformation to ensure analytical depth and allow for deeper consideration of case studies. It will incorporate case studies from various EU member states, particularly the Baltic states of Estonia, Latvia and Lithuania, which have historically been at the forefront of resisting and countering Russian-backed disinformation campaigns. Consequently, this article advances the argument that the EU's role in strengthening resilience against hybrid warfare must take a whole-of-society approach, along with facilitating international and inter-institutional cooperation and establishing common standards to mitigate vulnerabilities.

The nature of hybrid threats and vulnerabilities

Hybrid threats

Since Russia's interference in the 2016 US elections and the Cambridge Analytica scandal, there has been a growing awareness of hybrid threats and foreign interference in democratic processes in Western political and academic circles. These developments have also spawned a rapidly growing research agenda on 'hybrid warfare', to the extent that some scholars have now begun to view this term as a buzzword and question its analytical utility (Bērziņš 2020; Renz 2016; Hartmann 2017, 1; Van Puyvelde 2015). The purpose of this article, however, is not to contribute to these conceptual debates, but rather to examine the EU's resilience capabilities from institutional, regulatory and societal perspectives. Therefore, the article treats 'hybrid threats' as an umbrella term that covers a range of destabilising and synchronised civil and military actions (Fiott and Parkes 2019; Szymanski 2020, 2; Heap 2020, 18). These activities can include disinformation campaigns, cyberattacks, inducing political or economic corruption, infiltrating agents of influence, pressuring independent media and buying up critical infrastructure (Hybrid CoE 2019, 10).

Moreover, it should, from the outset, be clarified that countering hybrid threats is primarily the competence and responsibility of member states. Unlike the EU or other international organisations, national governments have the requisite tools, including 'intelligence and counterintelligence agencies (both civilian and military), uniformed services (ensuring public order and safety), means of communication with citizens and cyber incident response capabilities' (Szymanski 2020, 2), to directly counter hybrid threats. At the same time, while national security falls under the purview of each member state's vital interest, hybrid threats often transcend borders, leaving a critical complementary role to be filled by the EU in support of member states' efforts (Dunay and Roloff 2017). In other words, the EU (and NATO) can play a key subsidiary role and offer resilience support in instances where member state responses at the national level have proven inadequate (Szymanski 2020, 2).

Russian foreign interference

The effectiveness of Russia's interference through hybrid warfare can be explained in terms of its ability to identify and exploit vulnerabilities inherent to our democratic societies. By their very nature hybrid threats are multifaceted, ambiguous and covert, rendering them very difficult to deter, identify, counter or attribute (Heap 2020, 8). Crucially, the aim of hybrid warfare is not to directly confront or attack the target, thus eliciting an immediate reaction, but rather 'to weaken its resolve by covert means of interference calibrated to undermine its internal cohesion' (Wigell 2019, 262). Moreover, technological developments are happening at an ever-growing pace, often restricting our capability to identify malicious practices *post factum*. The evolution of the available tools increases the reach and effectiveness of hybrid warfare in the pursuit of strategic objectives such as undermining public trust in institutions, gaining geopolitical influence and hampering institutional decision-making capabilities (Hybrid CoE 2019, 10).

Furthermore, the effectiveness of such tactics hinges on their ability to exploit the core principles, laws and values that govern democratic societies. Russia's deployment of hybrid tools, such as disinformation campaigns, targets the inherent vulnerabilities of open and democratic systems, such as freedom of speech, freedom of the media and freedom of the markets, among others. These freedoms all represent potential avenues for foreign interference. The open pluralism of European democracies has and continues to be exploited to exacerbate existing ethnic, religious, political or economic fault-lines, thereby undermining societal cohesion. Hybrid threats thus represent a highly effective 'wedge strategy'—a tactic aimed at fomenting polarisation and radicalisation to the point that the principles of democratic societies are stretched to their extremes (Wigell 2019, 270). Critically, once this wedge has been driven and societal cohesion has been undermined, the stage is set for further potentially escalatory hybrid activities that exploit this turmoil and lack of unity (Wigell 2019, 256). Several prominent instances of Russia's use of wedge strategies in EU member states have involved Russian-backed social media troll and bot campaigns seeking to foment anger and polarisation amidst the ongoing COVID-19 crisis response (EEAS 2020), as well as during the Brexit referendum in the

UK (Kirkpatrick 2017), the *Gilets jaunes* (Yellow Jackets) protests in France (Coffey 2019) and the protests for Catalonian independence in Spain (Emmott 2017).

Resilience

Finally, it is necessary to briefly establish what is understood by the term 'resilience'. As evidenced by the emergent body of research on hybrid threats, the concept of resilience has also acquired numerous definitions and subsequent applications. For the purposes of this article, resilience is understood to represent the ability of states and societies to deter, resist and overcome the impact of external interference, particularly in terms of demonstrating institutional capacity, good governance and societal cohesion (Dunay and Roloff 2017). As outlined by a report from the NATO Strategic Communications Centre of Excellence: 'Improving overall resilience requires addressing vulnerabilities and taking a long-term approach to build strong and adaptive infrastructure, ensure social cohesion and sustain trust in government. Resilience not only mitigates the harmful effects of hostile influence, but it can also change the adversary's overall cost–benefit calculation' (Heap 2020, 12). Additionally, in the case of the EU and its member states, resilience measures must always respect the fundamental democratic values and freedoms that their societies are built upon.

Institutional resilience measures

Adaptation of political and legal frameworks

The institutional dimension of the Union's resilience to hybrid warfare is critical to signalling that there is the political will to take these threats seriously. Therefore, it is necessary to first look at the steps that the EU institutions have undertaken to build their capacity to counter hybrid threats. Since 2014, the EU has adopted a range of legislation in this field, including in policy areas such as energy security, safeguarding of critical infrastructure, data protection, screening of foreign investments and transparency of political funding, among others (Fiott and Parkes 2019; Szymanski 2020, 3). To outline some of the key initiatives, first, in April 2016, the European Commission introduced the Communication *Joint Framework on Countering Hybrid Threats*, which is integral to structuring the EU's activities in this domain (European Commission 2016). Second, in June 2018, the Commission published the *Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats* (European Commission 2018b). Third, the EU's new strategic agenda for 2019–24 explicitly highlights resilience to hybrid threats and disinformation as one of the key future areas of work (European Council 2019a; Bajarūnas 2020, 64). Finally, in December 2019, the European Council Conclusions on countering hybrid threats were adopted, which were historic due to their reference to 'the possibility for the Member States to invoke the Solidarity Clause (Article 222 TFEU) in addressing a severe crisis resulting from hybrid activity' (Council of the EU 2019, 6).

Establishment of new institutions

Beyond providing an institutional framework and political–legal basis for the EU's hybrid resilience measures, several institutional initiatives have produced tangible results on the ground. In 2016, recognising the need to advance European capabilities in hybrid threat analysis and information sharing, the EU established a Hybrid Fusion Cell as part of the EU Intelligence and Situation Centre. This body has served as an important supplementary instrument, providing threat analysis and data collection on hybrid activities targeting EU member states and the neighbourhood (Szymanski 2020, 5; Bajarūnas 2020, 65). Furthermore, after a protracted bureaucratic process, projects aimed at countering hybrid threats have been granted access to the European Defence Fund, ensuring a substantive budgetary basis to underpin the EU's political commitment. For its part, the European Parliament has also responded by setting up the Special Committee on Foreign Interference in All Democratic Processes in the EU, Including Disinformation (INGE). With a powerful political mandate and a high-profile political platform, the INGE committee has the potential to generate important visibility and political support for the EU's efforts to investigate and counter foreign interference, including through a series of hearings, testimony sessions and public debates. The INGE committee is due to present a report to the European Parliament containing factual findings and recommendations concerning the measures to be taken to prevent and deter third-state actors from interfering in the functioning of democracy in the EU and its member states.

Moreover, a crucial component of the EU's institutional effort to deter and counter hybrid threats has been the establishment of three StratCom forces under the auspices of the European External Action Service (EEAS)—one focusing on the Eastern Partnership region, one on the Western Balkans and one on the Southern neighbourhood (Szymanski 2020, 6). The work of the EEAS StratCom forces in uncovering disinformation aimed at the EU in these regions represents a critical first step to raising the costs for the actors engaging in these activities (Fiott and Parkes 2019). Despite its highly limited budget and personnel, since 2015 East StratCom has reported and refuted over five thousand instances of disinformation spread by Russian-backed news operators on the subjects of COVID-19, the attempted poisoning of Alexei Navalny, the US military footprint in Europe, the migration crisis, Daesh, the Salisbury chemical weapons attack and the downing of flight MH17 (Gotev 2018). Furthermore, countries in the EU's neighbourhood, especially those harbouring aspirations of close Euro-Atlantic integration, have been frequent targets of Russian-sponsored disinformation. For instance, Georgia has been repeatedly targeted by Russian disinformation campaigns that claimed that a health security research facility set up with US support in Georgia was conducting experiments on the local population (Anjaparidze 2020). Furthermore, investment in the EEAS Stratcom capabilities demonstrates a commitment to the external dimension of countering hybrid threats. By assisting accession countries in the Western Balkans and aspiring potential candidates, such as Georgia, Moldova and Ukraine, to build resilience, the EU is not only strengthening democratic institutions in these countries, but also directly promoting its own security interests (Bajarūnas 2020, 68). In the light of this track record, it is clear that these newly established institutions should be further empowered by urgently addressing issues of underfunding and personnel deficits, as well as broadening their

mandate. In this regard, the European Parliament has pushed to reinforce the operational capacity of the East StratCom Task Force by including its budgetary resources in the EU's Multiannual Financial Framework, as opposed to allocating funding on an annual basis. The EEAS StratCom force would benefit immensely from an expanded mandate that includes further deterrence capabilities, including the ability to blacklist, publicly attribute or perhaps sanction the foreign actors behind disinformation.

Inter-institutional cooperation

Finally, there have been promising developments with respect to inter-institutional cooperation in building resilience to hybrid threats, notably exemplified through EU–NATO cooperation. The EU and NATO are natural partners in this sphere, operating with broadly similar strategic outlooks, risk assessments and interests in countering hybrid threats, particularly from Russia (Szymanski 2020, 1). In July 2016, the president of the European Council, president of the European Commission and secretary general of NATO signed a joint declaration outlining seven areas of cooperation, including the effort to counter hybrid threats (Tusk et al. 2016; Bajarūnas 2020, 64). A notable tangible development in EU–NATO cooperation has been the establishment of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in April 2017, which now includes 27 EU and NATO participant states. This organisation represents a pivotal investment in deepening trust and information exchange between the EU and NATO at the strategic level, expanding the EU's research and analytical capabilities, as well as organising joint exercises to strengthen preparation and resilience capabilities for countering hybrid interference (Bajarūnas 2020, 66).

Regulatory resilience measures

Beyond institutional adaptation to the growing potential of hybrid threats, the EU has sought to utilise regulatory instruments to limit the spread of disinformation, which compromises societal resilience by fomenting polarisation and radicalisation, and undermines trust in public institutions. In particular, the outsized role of large technology corporations, such as Facebook, Google and Twitter, and their algorithms has come under scrutiny, as news consumption has rapidly shifted to social media. Consequently, the power of large digital platforms has dangerously grown to encompass distinctly *political* functions, with their biased and profit-driven algorithms effectively moderating what content is released, shared and proliferated across the digital space without 'sufficient transparency, adequate fact-checking, journalistic values, and accountability to societies and audiences' (Hybrid COE 2019, 14). As demonstrated in the controversy surrounding the role of Cambridge Analytica in the 2016 US presidential election and the Brexit referendum, these opaque algorithms can be manipulated and exploited to perform a range of hybrid information operations that undermine the integrity of democratic processes. The non-transparent nature of the social media environment has also been repeatedly exploited by Russian-supported troll farms, including the notorious 'Internet Research Agency' linked to the pro-Kremlin oligarch Yevgeny Prigozhin (Stanford Internet Observatory 2019). These Kremlin-backed organisations have conducted far-reaching troll and bot campaigns, and created thousands of fake accounts, not only on social media networks but

also on discussion platforms, online media forums and video streaming services, seeking to polarise discussions and promote anti-Western narratives.

Under growing pressure to address this threat, the EU first released a Code of Practice to tackle disinformation in September 2018, which was hailed as the first worldwide framework for self-regulation aimed at curbing disinformation. The Code of Practice was signed by social networks and partners from the advertising industry. In December 2018, this step was complemented by the EU Action Plan for disinformation which was intended as a proactive measure to 'protect the Union's democratic systems and combat disinformation, including in the context of the upcoming European elections' (European Commission 2018a, 1). Within the scope of this plan, a Rapid Alert System was set up in March 2019, with the aim of facilitating rapid coordination of member states' responses to disinformation through an extensive network of national contact points (Hybrid CoE 2019, 15). While both of these initiatives were significant in demonstrating the EU's growing political will, both have shown notable limitations as the Code of Conduct is entirely voluntary and lacks any substantive enforcement or sanctions mechanism, while the Rapid Alert System remains severely under-utilised (Bajarūnas 2020, 65).

Nevertheless, in recognition of these flaws, there are encouraging signs that the EU will seek to become a standard setter in regulating the digital environment. At this time, two ambitious pieces of legislation are under discussion—the Digital Services Act, which will ensure greater consumer protection in the digital market, and the European Democracy Action Plan, which promises a revision of the regulations on the transparency of funding for European political parties and European political foundations. While there is serious resistance and lobbying expected from the influential big technology corporations, it is imperative that the EU avoids dilution of this legislation. Moreover, the EU's measures must be implemented as soon as possible, as further delays run the risk of individual member states implementing national legislation, thus creating the nightmarish scenario of a patchwork of 27 national frameworks. In sum, resilience to hybrid threats cannot be attained without an EU-wide set of norms to ensure accountability and transparency standards for online platforms.

Societal resilience measures

Having outlined the institutional and regulatory dimensions of the EU's approach to strengthening resilience to hybrid threats, it is also critical to consider the role of broader societal engagement. Hybrid threats are difficult to identify and counter, rendering strategic communications and the involvement of all sectors of society increasingly important. The need to increase societal resilience has also been amplified by other processes that have challenged democratic institutions and systems around the world. Indeed, recent years have witnessed an unmistakable 'democratic deconsolidation' (Wigell 2019, 274), marked by erosion of the rule of law, rollbacks of judicial independence and curtailing of the freedom of the press, not only around the world, but in several EU member states. The recent attack on the US Capitol is just one of numerous stark reminders of the vulnerability of democratic institutions and values. The EU needs to respond proactively.

Fortunately, the EU has the opportunity to draw on the expertise of 'front-line' member states, including the Baltic states, which have long faced the full arsenal of Russia's interference and disinformation attempts. Seeking to exploit Russian-speaking audiences in Latvia and Estonia, Russia has conducted information operations via social media, its state-owned television platforms and newspapers, and other agents of influence. In particular, Russian disinformation campaigns have sought to promote two central narratives. The first is that the Baltic states are rabidly nationalist, fascist failed states that have been on a trajectory of severe decline since joining the EU and NATO. The second claims that the EU, NATO and the US are exploiting the Baltic states as a launch pad for future aggression against Russia. In addition to these narratives, Russia is attempting to revise history and falsify historical memory, advancing the grand claim of a Russian geopolitical 'birth right' to a range of neighbouring countries and territories, including the Baltic states, Ukraine, Belarus, Georgia and Moldova, among others. The response of the Baltic states has centred on a whole-of-society approach that engages partners from the private sector, academia and the non-governmental sector. This outreach has contributed to the implementation of inclusive policymaking that is more attuned to the concerns and needs of the general population (Heap 2020, 31; Marovic 2019).

Effectively engaging civil society remains at the very core of the collective effort to strengthen societal resilience, including through efforts to 'support information pluralism, invest in civic awareness through education and maintain an independent press that responds swiftly to any disinformation' (Bajarūnas 2020, 68). In this regard, support for an independent and quality media must be a distinct priority, as journalists and the news media play a critical role in ensuring the integrity and operational capacity of democratic institutions and processes by providing reliable and trustworthy information as well as checking the power of policymakers (Hybrid CoE 2019, 11). A successful instance of such cooperation in the Baltic states has been the involvement of the investigative media outlet Re:Baltica in an official fact-checking capacity for Facebook, thus helping to identify and prevent the rapid, uncontrolled proliferation of harmful content (*Re:Baltica* 2020). The integral role of an independent media becomes especially clear during crises or states of emergency (as highlighted during the COVID-19 pandemic), when the need for verifiable, transparent information becomes even more pressing. For instance, several EU states have been the target of Russian-driven disinformation campaigns seeking to exploit the societal tensions stemming from the COVID-19 crisis, including by sowing doubts about the safety of Western-purchased vaccines and questioning the credibility of governments' response measures. Hence it is important to ensure the operational preconditions needed for the journalistic news media and their resilience to fake news and information harassment, as only an informed society can possess the necessary resilience to respond to a crisis or potential hybrid threat in a resolute and robust manner.

Conclusion

In conclusion, the EU has taken a range of notable steps to strengthen its resilience to hybrid threats from third countries in the information space, signalling a shift in awareness and a growing political will to take these threats seriously. While hybrid warfare can constitute a

broad array of activities, such as cyber-attacks, election interference and attacks on critical infrastructure, for the sake of analytical depth this article has focused on the EU's counter-disinformation efforts. It has engaged in a comprehensive examination of the EU's remaining vulnerabilities and potential future measures, in the process articulating the relevance of a whole-of-society approach to building resilience, drawing upon the resources of the independent media, the private sector, academia and non-governmental organisations. At the same time, critical vulnerabilities remain, further underscoring the need for proactive political engagement and resource allocation from the Union. Furthermore, we continue to see that close commercial links between several member states and Russia and the Kremlin's effective lobbying efforts continue to fragment the European Council's political will and unity on foreign and security policy. It is essential that the EU speaks and acts with one voice in its relations with Russia, particularly when it comes to defending fundamental values and countering foreign interference in its democratic processes.

Mapping the way forward, it is clear that the EU must pursue the following actions to strengthen its resilience to disinformation and interference in democratic processes:

1. Empower and broaden the mandate of its institutions that aim to counter disinformation in the EU and its neighbourhood.
2. Expand its investigations into foreign interference, including but not limited to disinformation, and publicly expose, sanction and deter those behind it.
3. Become a global standard-setter in regulating the digital single market, including demanding greater transparency and accountability from digital platforms. This includes the establishment of EU-wide general standards for social responsibility in algorithmic design.
4. Enforce greater scrutiny in monitoring foreign political funding and the financing of political advertising in the EU and its member states.
5. Involve civil society, academia and the non-governmental sector in a whole-of-society approach to countering disinformation.
6. Expand its activities in ensuring media safety and sustainable operation, countering censorship and media persecution, and empowering a quality and independent media.
7. Strengthen cooperation with NATO, the UN (especially UNESCO), the G7 and other like-minded international organisations and partners.

References

Anjaparidze, Z. (2020). Russia dusts off conspiracy theories about Georgia's Lugar Center laboratory in midst of COVID-19 crisis. *Jamestown Foundation*, 5 May. https://jamestown.org/program/russia-dusts-off-conspiracy-theories-about-georgias-lugar-center-laboratory-in-midst-of-covid-19-crisis/. Accessed 22 February 2021.

Bajarūnas, E. (2020). Addressing hybrid threats: Priorities for the EU in 2020 and beyond. *European View*, *19*(1), 62–70.

Bērziņš, J. (2020). The theory and practice of new generation warfare: The case of Ukraine and Syria. *The Journal of Slavic Military Studies*, *33*(3), 355–80.

Coffey, L. (2019). Russia exploits 'yellow vest' turmoil in France. *The Heritage Foundation*, 8 February. https://www.heritage.org/europe/commentary/russia-exploits-yellow-vest-turmoil-france. Accessed 22 February 2021.

Council of the EU. (2019). *Complementary efforts to enhance resilience and counter hybrid threats – Council conclusions*. 10 December. https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf. Accessed 22 February 2021.

Deutsche Welle. (2020). Georgian's death in Berlin was a Russian-ordered assassination, prosecutors believe. 18 June. https://www.dw.com/en/georgians-death-in-berlin-was-a-russian-ordered-assassination-prosecutors-believe/a-53860911. Accessed 22 February 2021.

Dunay, P., & Roloff, R. (2017). *Hybrid threats and strengthening resilience on Europe's eastern flank*. George C. Marshall European Center for Security Studies. March. https://www.marshallcenter.org/en/publications/security-insights/hybrid-threats-and-strengthening-resilience-europes-eastern-flank-0. Accessed 22 February 2021.

EEAS. (2020). Pro-Kremlin disinformation: COVID-19 vaccines. Delegation of the European Union to Azerbaijan. 22 December. https://eeas.europa.eu/delegations/azerbaijan/90950/pro-kremlin-disinformation-covid-19-vaccines_en. Accessed 22 February 2021.

Emmott, R. (2017). Spain sees Russian interference in Catalonia separatist vote. *Reuters*, 13 November. https://www.reuters.com/article/us-spain-politics-catalonia-russia-idUSKBN1DD20Y. Accessed 22 February 2021.

European Commission. (2016). *Joint framework on countering hybrid threats: A European Union response*. Joint Communication, JOIN (2016) 18 final (6 April).

European Commission. (2018a). *Action plan against disinformation*. Joint Communication, JOIN (2018) 36 final (5 December).

European Commission. (2018b). *Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*. Joint Communication, JOIN (2018) 16 final (13 June).

European Council. (2019). *A new strategic agenda, 2019–2024*. Brussels.

Fiott, D., & Parkes, R. (2019). *Protecting Europe: The EU's response to hybrid threats*. European Union Institute for Security Studies, Chaillot Paper 151.

Gotev, G. (2018). Experts lament underfunding of EU task force countering Russian disinformation. *Euractiv*, 23 November. https://www.euractiv.com/section/global-europe/news/experts-lament-underfunding-of-eu-task-force-countering-russian-disinformation/. Accessed 23 February 2021.

Hartmann, U. (2017). *The evolution of the hybrid threat, and resilience as a countermeasure*. NATO Defense College, Research Division.

Heap, B. (2019). *Hybrid threats. A strategic communications perspective*. NATO Strategic Communications Centre of Excellence.

Hybrid COE. (2019). *Countering disinformation: News media and legal resilience*. Hybrid CoE Papers.

Kent, G. (2020). Russia's MH17 web of lies looks set to unravel in court. *Atlantic Council*, 22 July. https://www.atlanticcouncil.org/blogs/ukrainealert/russias-mh17-web-of-lies-continues-to-unravel/. Accessed 23 February 2021.

Kirkpatrick, D. (2017). Signs of Russian meddling in Brexit referendum. *New York Times*, 15 November. https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html. Accessed 23 February 2021.

Marovic, J. (2019). *Wars of ideas: Hybrid warfare, political interference, and disinformation*. Carnegie Europe. 28 November. https://carnegieeurope.eu/2019/11/28/wars-of-ideas-hybrid-warfare-political-interference-and-disinformation-pub-80419. Accessed 22 February 2021.

Re:Baltica. (2020). Re:Check kļūst par oficiālajiem FB faktu pārbaudes partneriem. 25 March. https://rebaltica.lv/2020/03/recheck-klust-par-oficialajiem-fb-faktu-parbaudes-partneriem/. Accessed 22 February 2021.

Renz, B. (2016). Russia and 'hybrid warfare'. *Contemporary Politics*, *22*(3), 283–300.

Rettman, A. (2017). Illicit Russian billions pose threat to EU democracy. *EUObserver*, 21 April. https://euobserver.com/foreign/137631. Accessed 22 February 2021.

Sabbagh, D., Hardin, L., & Roth, A. (2020). Russia report reveals UK government failed to investigate Kremlin interference. *The Guardian*, 21 July. https://www.theguardian.com/world/2020/jul/21/russia-report-reveals-uk-government-failed-to-address-kremlin-interference-scottish-referendum-brexit. Accessed 22 February 2021.

Stanford Internet Observatory. (2019). *Evidence of Russia-linked influence operations in Africa*. Cyber Policy Center. https://fsi.stanford.edu/publication/evidence-russia-linked-influence-operations-africa. Accessed 22 February 2021.

Szymanski, P. (2020). Towards greater resilience: NATO and the EU on hybrid threats. *Centre for Eastern Studies*, OSW Commentary 328.

Tusk, D., Juncker, J.-C., & Stoltenberg, J. (2016). *Joint declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg*. https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf. Accessed 22 February 2021.

Van Puyvelde, D. (2015). Hybrid war: Does it even exist? *NATO Review*. https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html. Accessed 22 February 2021.

Wigell, M. (2019). Hybrid interference as a wedge strategy: A theory of external interference in liberal democracy. *International Affairs*, *95*(2), 255–75.

Author biographies

Sandra Kalniete *is a Member of the European Parliament from Latvia in the Group of the European People's Party. She is a member of the Parliament's Committee on Foreign Affairs, the INGE Committee, the Delegation to the EU–Ukraine Parliamentary Association Committee and the Delegation to the Euronest Parliamentary Assembly.*

Tomass Pildegovičs *is a policy assistant to Sandra Kalniete and a Ph.D. candidate in politics and international relations at the University of Cambridge. He completed his M.Phil. in international relations and politics with distinction at the University of Cambridge in 2019. Pildegovičs also holds a BA in international relations with first class honours (2018) from the Department of War Studies, King's College London.*