European Union Institute for Security Studies

FEELING THE PULSE

BRIEF / 18
Oct 2023

Countering foreign information manipulation and interference in Africa and the Western Balkans

The EUISS is an agency of the European Union

by

Tijana Morača
Senior Researcher, University of Milano-Bicocca

Federico Giulio Sicurella
Senior Researcher, University of Milano-Bicocca

Tatjana Sekulić
Associate Professor, University of Milano-Bicocca

Justin Armanini
Data Analyst, University of Milano-Bicocca

Fabio Antonio Stella
Associate Professor, University of Milano-Bicocca

Summary

- Foreign information manipulation and interference (FIMI) represents a serious challenge to the EU's global interests and values.
- As evidence from the Western Balkans and African contexts shows, the line between foreign and domestic information manipulation is often blurred. The EU's presence and objectives in partner countries can also be seriously threatened by information activities that do not necessarily qualify as malign, intentional or coordinated.
- The ability to 'feel the pulse' of the information environment – by refocusing the analysis of FIMI beyond the foreign-domestic dichotomy and narrowly defined intention and coordination – can help the EU improve its situational awareness, develop better-targeted counter-FIMI responses and enhance strategic communications.

INTRODUCTION

Foreign information manipulation and interference (FIMI) has increasingly come into the spotlight of EU policies aimed at countering disinformation. The European External Action Service[1] has recently applied the concept to detect and analyse manipulative information activities by Russian and Chinese actors, with promising results, substantiating the value of

Funded by the European Union

Countering Foreign Interference

FIMI's focus on potential harm to the EU's own political processes and values. Yet, the question arises as to how to best leverage FIMI – as an emerging policy and analytical concept – to enhance EU engagement in partner countries.

This Brief argues that, by focusing only on outright cases of foreign-led, intentional and coordinated information manipulation in third-country information spaces, the EU risks missing critical vulnerabilities and potential threats to its own standing and objectives worldwide. In particular, the authors draw on cases from the Western Balkans (WB) and selected African countries[2] – two contexts where the EU's strategic interests[3] are increasingly at stake due to the growing presence of competing actors such as Russia and China. The authors demonstrate how the line between foreign and domestic information activities is not always clear-cut, and how media narratives with the potential to undermine the EU often escape strict definitions of malign behaviour.

In response to these challenges, broadening the focus of the FIMI concept beyond the foreign-domestic dichotomy and narrowly defined intention and coordination can have significant impact. The ability to 'feel the pulse' of the wider information environment, the Brief concludes, is crucial to assessing and effectively responding to potential FIMI threats to the EU's external presence and strategic communication.

The Brief consists of four sections. The first explains what FIMI is and why it has become a challenge to the EU's external action. The second focuses on the foreign-domestic nexus in the information space, pointing to the need to transcend the foreign-domestic dichotomy when dealing with FIMI. The third section shows how FIMI often successfully exploits existing narratives and trends, arguing in favour of extending the scope of FIMI analysis to information activities that may not be explicitly intentional or coordinated, and that do not seem to target EU actors directly[4]. In the conclusion, the main points are recapitulated and translated into recommendations for policymakers.

The EU's space for proactive strategic communication is shrinking due to increasingly hostile information environments.

The EU's Strategic Compass for Security and Defence was adopted in March 2022.

European External Action Service

FIMI AS A CHALLENGE TO THE EU'S GLOBAL ENGAGEMENT

In its most recent and widely accepted definition, FIMI refers to 'a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes, [which is] manipulative in character, conducted in an intentional and coordinated manner, [and whose agents] can be state or non-state actors, including their proxies inside and outside of their own territory'[5]. As a policy concept, FIMI has found ground in the profound restructuring that the EU's security architecture has undergone over the past decade, following critical developments such as Russia's illegal annexation of Crimea in 2014, Russian meddling in the 2016 presidential elections in the United States, the Covid-19 pandemic and, most evidently, the ongoing Russian aggression against Ukraine. The 2022 *Strategic Compass for Security and Defence* defines these dramatic changes as the return of war and power politics in Europe – both in the conventional geopolitical sense and in increasingly contested domains, including the cyber sphere – and advocates for a common European posture in the face of novel threats to 'human rights, human society and democratic values [...] both at home and abroad'. The EU, it concludes, faces a 'real battle of narratives'[6].

Over the past decade, the EU has engaged in the production of new conceptual, legal and practical frameworks to strengthen its capacity to anticipate, mitigate and respond to threats of information manipulation. While the EU's initiatives in this field have mostly focused on information manipulation targeting democratic decision-making processes *within* the EU and its Member States, FIMI has been increasingly recognised as a serious challenge to the EU's external action and global engagement as well. Indeed, FIMI appears to systematically erode the EU's strategic presence in partner countries, while its space for proactive strategic

communication is shrinking due to increasingly hostile information environments[7].

Existing research focusing on the EU's Common Security and Defence Policy (CSDP) missions and operations has shown that their activities are occasionally exploited by FIMI actors in the context of broader campaigns intended to undermine the EU and its allies[8]. Clearly, while FIMI may harm the reputation of individual missions, one of its primary dangers lies in its capacity to damage local acceptance of the EU's presence more generally. Local media spaces that can be volatile and polarised compound this risk. So too does the lack of capacity on the part of the missions to systematically analyse media content and assess specific FIMI threats[9]. Together, these factors create easy opportunities for FIMI actors to control the narrative and influence target audiences.

In sum, foreign-led information manipulation has the potential to undermine the EU's foreign and security policy priorities. That raises the question of how best to leverage FIMI as an analytical concept and emerging policy framework, both to enhance the EU's leading role in the global battle against information manipulation and to strengthen EU partner countries' own resilience and capacity to respond to FIMI threats.

FIMI actors have learned to exploit the symbiotic relationship between domestic and foreign information activities.

BEYOND THE FOREIGN-DOMESTIC DICHOTOMY

FIMI refers to foreign information activities, as opposed to domestic ones. The policy relevance of this distinction is significant: not only does it reflect the different mandates of EU institutions dealing with information manipulation, it also provides common ground for the EU and its strategic allies to define and engage effectively with the problem. However, drawing a clear-cut line between foreign and domestic information activities might pose some limitations, both analysis- and policy-wise.

The blurred line between domestic and foreign: Evidence from African information environments

Academic research into disinformation has greatly emphasised how domestic and foreign information activities, including adversarial and manipulative ones, are in a symbiotic relationship. They tend to be closely associated in mutually beneficial ways that are often difficult to untangle[10].

Empirical research conducted in African contexts has provided robust evidence of such symbiosis, which often rests on a convergence of political and economic interests between local elites and foreign actors. In Sudan, during the protests in January 2019, state-linked media channels and Russian media were aligned in presenting the turmoil as an attempt by foreign powers to destabilise the country[11]. In Mali, a deteriorating security situation has facilitated the proliferation of a 'fake news' ecosystem[12] in which politicians and government officials actively sponsor Russian-sourced propaganda to serve their own ends. A similar trend occurred in the Central African Republic, where the government has been accused of engaging in Russian-backed disinformation campaigns targeting domestic civil society, French diplomats and the United Nations peacekeeping mission[13].

FIMI actors have learned to exploit the symbiotic relationship between domestic and foreign information activities. Russia's information manipulation across Africa, for instance, relies on systematic orchestration of Russian-owned international outlets and domestic media channels, blending local content with pro-Russian and anti-Western material[14]. What is more, specific FIMI strategies not only exploit but also reinforce the convergence between domestic and foreign information activities. Using or posing as local voices to project authenticity is one of them. Researchers have identified cases of foreign-linked media channels posing as local voices[15] in Mali[16] and the Central African Republic[17], among other places. Tactics such as franchising, subcontracting or 'sock-puppeting' are aimed at creating a perception of authentically local, multi-sourced and pluralistic journalism, while they in fact entrench echo chambers of support for certain foreign actors.

On top of this, there are strong economic incentives for local media to relay foreign-sourced content. Domestic media houses can stretch limited budgets by relaying content that foreign state media make readily (and often freely) available via syndication, rather than buying content from international news agencies. In several African countries, Russian media content is massively shared, quoted and discussed at the community level, to the point that Russian sources have *de facto* become an integral part of local media and information spaces[18].

With the boundaries between foreign and domestic information activities increasingly blurred, FIMI actors are incentivised to deploy strategies and tactics that leverage and further cement this ambiguity. This is why the EU's ability to identify, analyse and assess

potential FIMI threats in partner countries' information environments will be strengthened by focusing beyond media sources that can be attributed to foreign actors, such as state-controlled or state-run media and their known proxies.

Why domestic information manipulation should not be overlooked: The case of the Western Balkans

Limiting the scope of counter-FIMI efforts to foreign information activities overshadows the extent to which domestic information manipulation can compound vulnerability to external influence.

The Western Balkan (WB) region offers a case in point. While there is ample evidence that Russia has succeeded in spreading its messaging across the region [19], in-depth research has shown that most disinformation content circulating in the WB media space is actually locally sourced. A 2021 study [20] reviewed 74 confirmed disinformation campaigns conducted across six WB countries up to 2020, and found that the majority of them consisted of domestic information activities, whereby disinformation was instrumentalised to achieve internal political objectives and undermine opponents. On the whole, the disinformation landscape was found to change depending on local political constellations. In Serbia and Montenegro, the cohesive nature of information manipulation and the interwoven narratives reflected the concentration of political power. Conversely, in Albania, Kosovo and North Macedonia, the study found less coherent and shorter-lived disinformation campaigns serving a variety of competing political forces. Exposure to transnational information manipulation was most pronounced in Kosovo, Bosnia and Herzegovina (BiH) and North Macedonia, countries in which the ability to govern is bound up in broader geopolitical relations.

Any attempt at determining what qualifies an information activity as foreign interference may face complex questions of proximity, belonging and political allegiances.

On top of this, the WB region has also seen a surge in the use of the disinformation lexicon as a framing device to discredit and dismiss criticism from non-like-minded actors, a tendency also observed at a global level [21]. As a result, terms such as disinformation and fake news have lost their connection to the facticity of information and are increasingly used as labels denoting partisan alignment. Such instrumental use of the disinformation lexicon in political parlance and media discourse may have direct repercussions on the EU's standing in contexts where the EU is perceived as threatening to local political elites.

When rooted in domestic political and media discourse, information manipulation and its weaponisation intensify the vulnerabilities of the information environment, and thus undermine its resilience to foreign interference. Therefore, it is essential to look at locally sourced (and locally targeted) information manipulation and its instrumentalisation in EU partner countries to foster the EU's capacity to form situational awareness of the threat landscape.

The issue of foreignness in FIMI

The FIMI concept places emphasis on the *foreign* dimension of information manipulation and interference. This begs questions of definition and positioning: what is foreign? Foreign to whom? This further raises potential issues for effective application of the FIMI framework in external contexts of strategic interest to the EU.

First, the *foreign* category seems to have limited analytical value in contexts where the boundaries of the information environment transcend national borders. Contemporary media spaces tend to be highly porous, with content being appropriated and amplified across national borders. This makes any assessment of the legitimacy of information activities based on the logic of sovereign national territory inherently incomplete [22]. Second, any attempt at determining what qualifies an information activity as *foreign,* or indeed as *foreign interference*, may face complex questions of proximity, belonging and political allegiances.

The WB region (with the addition of Croatia due to linguistic proximity [23]) offers a striking illustration of both points. To begin with, the porousness of the regional media space is immediately evident: shared languages allow for almost direct uptake and fusion of content – including false and manipulative content [24] – across country borders. This happens to the extent that it becomes extremely difficult to draw a clear line between domestic and foreign information activities. More importantly, in some countries in the region, significant segments of the population identify with ethnic groups that are the majority in neighbouring states. These individuals may not perceive content or media actors associated with these groups as foreign, or at least not as entirely or fundamentally so.

In such contexts, where content is almost by default appropriated transnationally, and the distinction between domestic and foreign is contextual and fluid, the applicability of the label *foreign* or *foreign interference* to certain information activities becomes less straightforward than it might appear.

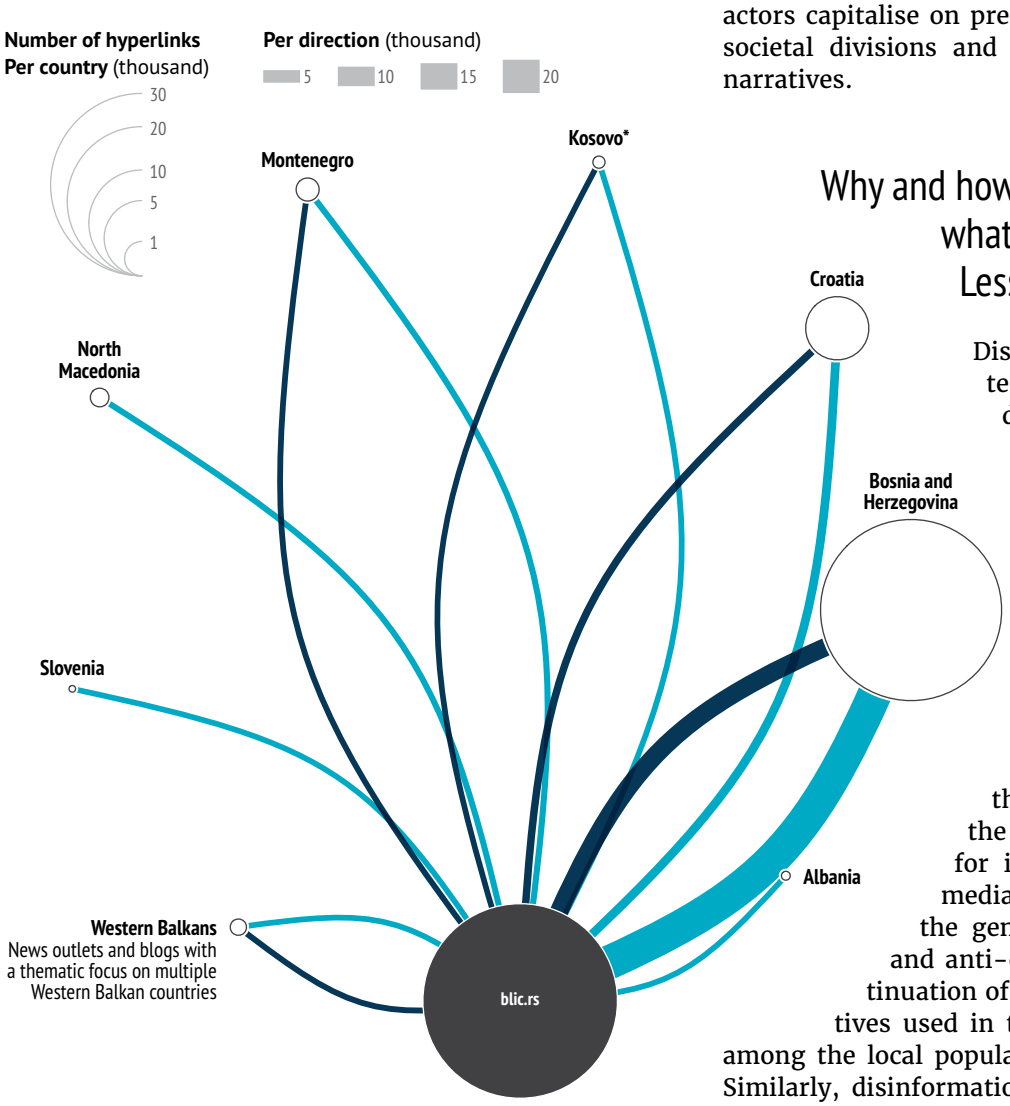
This complexity is also common in cases where a shared sense of historical proximity or political loyalty transcends existing geographical distance and linguistic barriers. WB and African contexts are particularly sensitive areas in this respect. For example, Russia tends to be favourably perceived among some segments of the population in the WB region, but is a paramount threat actor for the EU in terms of foreign information manipulation. Similarly, in several African countries the ability to diversify partnerships – including with Russia or China – is often perceived or represented as a key matter of national autonomy and post-colonial emancipation.

In such contexts, labelling information activities conducted by or linked to these actors as *foreign interference*, even when they meet the criteria of the EU's definition of FIMI, will likely collide with allegiances of proximity and political loyalties, and thus risks sparking opposition from some segments of the political establishment and the mass audience. This would represent a major obstacle to reaching a shared understanding of FIMI, and hence to building resilience and devising responses to external information manipulation and interference in the relevant EU partner countries.

Information environments transcend national borders

The case of Serbian news outlet blic.rs

To show the transnational character of the information ecosystem, this graphic represents the number of hyperlinks **from Serbian portal blic.rs** to news outlets from other countries of the Western Balkans, Croatia and Slovenia, and **from those outlets to blic.rs**, grouped by country.



Data: Storyzy, 2023 (extracted on 4 September 2023 and processed by the authors).

* This designation is without prejudice to positions on status, and is in line with UNSCR 1244 (1999) and the ICJ Opinion on the Kosovo declaration of independence

BEYOND MALIGN INTENTION AND COORDINATION

FIMI, influence operations and disinformation campaigns are mostly designed to sow discord and distrust in the target countries. To achieve this, malign actors capitalise on pre-existing contentious issues, societal divisions and deep-seated grievances and narratives.

Why and how FIMI exploits what's already there: Lessons from Africa

Disinformation campaigns often seek to mobilise broad, deep-seated narratives and fit them into existing polarising political issues. This has been confirmed in relation to the EU's engagement in the Eastern Partnership and the Sahel[25]. Recent analysis of Russian information manipulation across African countries provides further evidence. In Mali and the Central African Republic, for instance, Kremlin-sponsored media appear prone to mobilising the general theme of anti-Western and anti-colonial narratives as a continuation of mass communication narratives used in the Soviet era, whose appeal among the local population seems undiminished[26]. Similarly, disinformation strategists have leveraged the long tradition of the African non-aligned movement, particularly with regard to the Russian invasion of Ukraine, using non-alignment narratives to

amplify grassroots refusal to side with the West in what is cast as a bipolar, ideological war[27].

An additional case in point is the strand of post-colonial narratives known as *Afrancaux News*[28], which permeate contemporary fake news stories accusing French counterterrorism of destabilising the Sahel. *Afrancaux News* appears to have played a significant role in Russia's quest for greater influence[29]; for instance, when popular protests erupted in Mali in 2020, Russia readily instrumentalised them by launching a large-scale disinformation campaign accusing France of neocolonial meddling in Malian internal affairs, and the UN of occupying the country and supporting terrorist groups[30].

Based on these insights, it is beyond doubt that foreign information manipulation efforts largely incorporate and exploit 'homemade' narratives, that is, narratives that are not foreign-planted but rather form an integral part of the target country's information space. What is more, it is reasonable to assume that the more they do so, the greater their impact on target audiences is likely to be[31].

Foreign information manipulation efforts largely incorporate and exploit 'homemade' narratives.

Media narratives as indirect communication threats: Examples from the Western Balkans

Driven by the ambition to achieve a degree of objectivity in determining the malicious nature of foreign interference, the counter-FIMI community has placed growing emphasis on the notions of intention and coordination, leading to a shift in focus from analysis of content to a behaviour-first approach[32].

Detection of coordinated and covert manipulative activities in the information space (including foreign-orchestrated ones) can sometimes be quite effective. Looking at the WB context, for example: in March 2020 Twitter in Serbia took down a network of accounts acting in concert to support the ruling party and the president[33]; soon afterwards, the botnet still appeared to be active, working mainly to promote Chinese aid and to cheer for the Serbian government in the frame of the Covid-19 pandemic[34].

However, it tends to be extremely difficult to draw a clear distinction between information activities that are intentionally orchestrated (either by domestic or foreign actors) and those that are not. Moreover, in the WB media space, hostile or negative coverage only appears to *directly* target the EU to a limited extent[35]. Nevertheless, even when there is no clear malign intentionality, narratives and messaging circulating in the information environment might still pose an indirect threat to the EU's standing in the communication space, as well as exacerbate vulnerability to FIMI.

A salient case of anti-migrant messaging can serve to illustrate this point. In 2015, dozens of portals in Croatia, Serbia, Montenegro and BiH – including a public broadcaster in the Republic of Srpska[36] – republished supposed testimony from an unidentified Czech doctor denouncing violence committed by migrants in a Munich hospital. The testimony, which was originally published by a conspiratorial Czech YouTube channel, turned out to be fabricated. The case might indicate some level of (possibly foreign-sourced) coordination: the YouTube channel was known to pick up Sputnik content[37], and the BiH public broadcaster that republished the content is considered to be part of the Sputnik ecosystem[38]. Furthermore, this specific story resonates with broader narratives in the WB media environments framing Europe, and by association the EU, as weak in the face of new challenges[39]. It remains extremely difficult, however, to determine whether and to what extent the circulation of such messaging is intentional and foreign-orchestrated. Rather, a myriad of motives and intentions – including commercial interests, authentic political beliefs and contestation, and foreign actors' interests – and their mutual entanglement are potentially at play in the diffusion and amplification of these and similar narratives.

Intention and coordination notwithstanding, narratives such as this have the potential both to indirectly undermine the EU's presence in contexts of interest, and to pave the way for potential FIMI. In this sense, focusing only on information incidents and campaigns that evidently fulfil the criteria of intentionality and coordination that define FIMI risks underestimating the threat landscape at large.

CONCLUSION AND RECOMMENDATIONS

This Policy Brief has examined how to best leverage FIMI as a policy and analytical concept to support the EU's external action and global engagement. Drawing on selected cases from WB and African contexts, the Brief has argued that, to strengthen the EU's capacity to assess and respond to the challenge of information manipulation targeting its presence and objectives in EU partner countries, its approach to FIMI should be enriched beyond the current focus on the foreign-domestic dichotomy, intention and coordination.

First, the Brief has showed how the foreign-domestic dichotomy is at odds with the reality of the analysed countries' information environments, where foreign and domestic information activities form interrelated ecosystems that FIMI actors have learned to exploit. Moreover, the authors conclude that any attempt at determining what qualifies an information activity as *foreign*, or indeed as *foreign interference*, may face complex questions of proximity, belonging and political allegiances.

Second, the Brief has demonstrated that a whole range of information activities that cannot be conclusively qualified as malign, intentional or coordinated – and which do not necessarily target EU actors directly – can still pose a significant threat to the EU's presence and objectives. In fact, the presence and circulation of narratives potentially favouring EU competitors, or promoting stances opposite to those the Union stands for, might still indirectly undermine the EU's standing in partner countries and provide opportunities for further exploitation by FIMI actors.

Drawing on these insights, the following five recommendations may enhance the EU's situational awareness and external engagement in the analysed partner countries:

1. The EU's approaches to assessing an information environment's threat landscape should be complemented with a focus that transcends, or at least carefully reconsiders, the dichotomy between foreign (and foreign-linked) and domestic information activities whereby *foreign* is understood as a precondition for information activity to be considered a threat.
2. The EU could carefully assess and contextualise its use of the term 'foreign' or 'foreign interference' in addressing information manipulation and when building counter-FIMI capacities of partner countries. Indeed, the labels *foreign* or *foreign interference* in FIMI may conflict with perceptions of belonging, proximity and political loyalties.
3. EU policymakers should additionally reconsider the foreign-domestic nexus and complement it with transnational analysis in contexts of shared language environments, where media content normally circulates across national borders.
4. The EU could expand the scope of FIMI analysis and assessment from its current focus on clear-cut malign information activities – i.e. intentional and coordinated incidents and campaigns, including those directly targeting specific EU bodies or the EU as a whole – to a broader focus on the wider media conversation on topics that bear relevance to EU values and objectives. This effort would benefit from further development of methodologies for narrative analysis that could be used to track critical content over time (as well as its potential transformation or re-appropriation for hostile purposes).
5. In any given context, understanding underlying societal vulnerabilities and geopolitical relations can complement information environment monitoring and assessment and benefit the EU's external action. The EU's strategies and support to local capacities can identify and capitalise on factors that may increase resilience to foreign interference.

In conclusion, the capacity to systematically 'feel the pulse' of the broader information environment – going beyond the narrow boundaries of foreignness, malign intent and coordination – is key to assessing and responding effectively to emerging challenges to the EU's external action and global engagement.

References

* This Policy Brief has been produced as part of the Countering Foreign Interference (CFI) project. The project is funded by the Foreign Policy Instruments (FPI) service of the European Commission, and carried out in cooperation with the European External Action Service (EEAS).

(1) European External Action Service, 'First EEAS report on foreign information manipulation and interference threats', February 2023 (https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en).

(2) In line with DG NEAR's conceptualisation of the Western Balkans in the latest EU Enlargement Package of 2022 (https://ec.europa.eu/commission/presscorner/detail/%20en/ip_22_6082).

(3) The EU has made important commitments and efforts in both areas, with WB countries being on the path to EU integration and the African continent being home to several EU missions and operations.

(4) The second and third sections are organised into sub-sections, each elaborating different aspects of the argument by drawing on material from either one of the two contexts of interest, i.e. Western Balkans and Africa.

(5) 'First EEAS report on foreign information manipulation and interference threats', op.cit.

(6) Council of the European Union, *A Strategic Compass for Security and Defence*, March 2022 (https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf).

(7) Huisman, C., 'A policy response to foreign information manipulation's impact on civilian CSDP missions', Center for International Peace Operations, 11 July 2022 (https://tech-blog.zif-berlin.org/sites/zif-tech-blog.org/files/inline-files/TECHPOPS-PDF-Crista%20Huisman-220711.pdf).

(8) Fridman, O., Baudais, V., and Gigitashvili, G., 'Enhancing the capabilities of CSDP missions and operations to identify and respond to disinformation attacks', European Parliament, February 2023 (https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702578/EXPO_IDA(2023)702578_EN.pdf).

(9) Ibid.

(10) See: Benkler, Y., Faris, R. and Roberts, H., *Network Propaganda: Manipulations, disinformation, and radicalization in American politics*, Oxford University Press, New York, 2018; Woolley, S.C. and Howard, P.N. (eds), *Computational Propaganda: Political parties, politicians, and political manipulation on social media*, Oxford University Press, New York, 2019; Hameleers, M., 'Disinformation as a context-bound phenomenon: toward a conceptual clarification integrating actors, intentions and techniques of creation and dissemination', *Communication Theory*, Vol. 33, No 1, 2022, pp. 1–10.

(11) Svoboda, K., Matlach, P.C. and Baddorf, Z., 'Russia's activities in Africa's information environment. Case studies: Mali and Central African Republic', NATO Strategic Communications Centre of Excellence, 2021 (https://stratcomcoe.org/publications/russias-activities-in-africas-information-environment-case-studies-mali-central-african-republic/6).

(12) Ouedraogo, L., 'Mali's fake news ecosystem. An overview', Centre for Democracy and Development, 2022 (https://africaportal.org/wp-content/uploads/2023/06/Fake-News-Mali-2.pdf).

(13) Ferebee, B. and Sullivan, R., 'Beyond fake news: the Central African Republic's hate speech problem', United States Institute of Peace, 2021 (https://www.usip.org/publications/2021/08/beyond-fake-news-central-african-republics-hate-speech-problem).

(14) See: Faleg, G. (ed.), 'African spaces: The new geopolitical frontlines', *Chaillot Paper* No 173, EUISS, March 2022 (https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_173_0.pdf); Soufan Center, 'Russian disinformation in an African context', *Intelbrief*, 7 November 2019 (https://thesoufancenter.org/intelbrief-russian-disinformation-in-an-african-context/).

(15) This is typically achieved by outsourcing publishing or posting operations to 'franchised' local influencers who are supplied content from a central source – a tactic that Wagner has used extensively in Africa. See: Africa Center for Strategic Studies, 'Mapping disinformation in Africa', 26 April 2022 (https://africacenter.org/wp-content/uploads/2023/02/Mapping-Disinformation.pdf).

(16) Ouedraogo, L., 'Mali's fake news ecosystem: An overview', Centre for Democracy and Development, 2022 (https://africaportal.org/wp-content/uploads/2023/06/Fake-News-Mali-2.pdf).

(17) Grossman, S., Bush, D. and DiResta, R., 'Evidence of Russia-linked influence operations in Africa', Stanford Internet Observatory, 29 October 2019 (https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf).

(18) See: Limonier, K., 'The dissemination of Russian-sourced news in Africa: A preliminary general map', IRSEM, 29 January 2019 (https://www.irsem.fr/data/files/irsem/documents/document/file/2965/RP_IRSEM_No66_2019.pdf); Mihoubi, S., 'La stratégie d'implantation de Radio Chine internationale (RCI) en Afrique sahélienne', *Norois*, Vol. 252, No 3, 2019, pp. 89–102 (https://journals.openedition.org/norois/9420).

(19) See: Bassuener, K., 'Pushing on an open door: Foreign authoritarian influence in the Western Balkans', National Endowment for Democracy, May 2019 (https://www.ned.org/wp-content/uploads/2019/05/Pushing-on-an-Open-Door-Foreign-Authoritarian-Influence-in-the-Western-Balkans-Kurt-Bassuener-May-2019.pdf).

(20) Greene, S., Asmolov, G., Fagan, A., Fridman, O. and Gjuzelov, B., 'Mapping fake news and disinformation in the Western Balkans and identifying ways to effectively counter them', European Parliament, February 2021 (https://www.europarl.europa.eu/RegData/etudes/STUD/2020/653621/EXPO_STU(2020)653621_EN.pdf).

(21) Tandoc, E.C. Jr., 'The facts of fake news: a research review', *Sociology Compass*, Vol. 13, No 9, p. 3.

(22) See: Ördén, H. and Pamment, J., 'What is so foreign about foreign influence operations?', Carnegie Endowment for International Peace, January 2021 (https://carnegieendowment.org/files/Orden_Pamment_ForeignInfluenceOps2.pdf); 'The dissemination of Russian-sourced news in Africa: A preliminary general map', op.cit.

(23) Roughly speaking, there are two groups of WB countries where linguistic proximity allows for content to be easily spread across borders: one comprises Serbia, BiH, Montenegro (with the addition of Croatia, and to some extent Slovenia), while the other includes Albania, Kosovo and North Macedonia.

(24) See, for example: Murić, D., Zulejhić, E., Živković, I., Janjić, S. and Radojević, V., 'Globalni narativi i lokalni akteri – 150 dana rata u Ukrajini i preko 1.500 dezinformacija u regionu', SEE Check, July 2022 (https://zastone.ba/app/uploads/2022/08/Globalni-narativi-i-lokalni-akteri-150-dana-rata-u-Ukrajini-i-preko-1.500-dezinformacija-u-regionu.pdf).

(25) Fridman, O., Baudais, V. and Gigitashvili, G., 'Enhancing the capabilities of CSDP missions and operations to identify and respond to disinformation attacks', European Parliament, February 2023 (https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702578/EXPO_IDA(2023)702578_EN.pdf).

(26) 'Russia's activities in Africa's information environment. Case studies: Mali and Central African Republic', op.cit.

(27) Otte-Witte, N., 'Disinformation on the front lines: "war is not just bombs and tanks"', DW Akademie, 4 May 2022 (https://akademie.dw.com/en/disinformation-on-the-front-lines-war-is-not-just-bombs-and-tanks/a-61681921).

(28) The term is a portmanteau that combines *Africa*, *France* and *faux* (*fake* in French).

(29) Kirwin, M., Ouedraogo, L. and Warner, J., 'Fake news in the Sahel: Afrancaux news, French counterterrorism, and the logics of user-generated media', *African Studies Review*, Vol. 65, No 4, pp. 911–938.

(30) Audinet, M., and Dreyfus, E., 'La Russie au Mali. Une présence bicéphale', IRSEM, September 2022 (https://www.irsem.fr/media/etude-irsem-97-audinet-dreyfus-def.pdf).

(31) Evidence of the reverse relationship, i.e. that narratives that do *not* speak to local interests are unlikely to achieve significant impact, is found in recent analysis of Russian propaganda in Africa: despite massive disinformation campaigns, Russia was unable to sway African countries to support its invasion of Ukraine. See: Blankenship, N. and Uche Ordu, A., 'Russia's narratives about its invasion of Ukraine are lingering in Africa', Brookings, 27 June 2022 (https://www.brookings.edu/blog/africa-in-focus/2022/06/27/russias-narratives-about-its-invasion-of-ukraine-are-lingering-in-africa/).

(32) 'First EEAS report on foreign information manipulation and interference threats', op.cit.

(33) Bush, D., '"Fighting like a lion for Serbia": an analysis of government-linked influence operations in Serbia (TAKEDOWN)', Stanford Internet Observatory, 2 April 2020 (https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/serbia_march_twitter.pdf).

(34) Digital Forensic Center, 'A bot network arrived in Serbia along with coronavirus' (https://dfcme.me/en/dfc-finds-out-a-botnet-arrived-in-serbia-along-with-coronavirus/).

(35) A 2019 study of the BiH information space shows that the EU was mentioned mainly neutrally and positively, while outright negative mentions were rare. See: Cvjetićanin, T, Zulejhić, E., Brkan, D. and Livančić-Milić, B., 'Disinformation in the online sphere – The case of BiH', Citizens' Association "Why Not"', April 2019, pp. 45–46 (https://zastone.ba/app/uploads/2019/05/Disinformation_in_the_online_sphere_The_case_of_BiH_ENG.pdf). Furthermore, a 2021 review of disinformation campaigns across the WB information space found that, despite the presence of narratives potentially damaging the EU brand, overall the EU was rarely thematised in the detected manipulative activities. See: 'Mapping fake news and disinformation in the Western Balkans and identifying ways to effectively counter them', op.cit., pp. 83–94 .

(36) See: Cvjetićanin, T., 'Kako je "vijest" sa Youtube-a završila na javnom servisu RS', Raskrinkavanje, 1 August 2018 ('https://raskrinkavanje.ba/analiza/kako-je-vijest-sa-youtube-a-zavrsila-na-javnom-servisu-rs).

(37) P. V., 'Ovaj čovjek je proširio lažne tvrdnje o ponašanju migranata u njemačkim bolnicama', Faktograf, 28 November 2019 (https://faktograf.hr/2019/11/28/ovaj-covjek-je-prosirio-lazne-tvrdnje-o-ponasanju-migranata-u-njemackim-bolnicama/).

(38) Cvjetićanin, T., Zulejhić, E., Brkan, D., and Livančić-Milić, B., 'Disinformation in the online sphere – The case of BiH', Citizens' Association 'Why Not', April 2019 (https://zastone.ba/app/uploads/2019/05/Disinformation_in_the_online_sphere_The_case_of_BiH_ENG.pdf).

(39) For the Western Balkans, see: Bechev, D., 'Russia's strategic interests and tools of influence in the Western Balkans', NATO Strategic Communications Centre of Excellence, 5 December 2019 (https://stratcomcoe.org/cuploads/pfiles/russias_strategic_interests_in_balkans_11dec.pdf); Atlantic Council of Montenegro, 'Russia's narratives toward the Western Balkans: analysis of Sputnik Srbija', NATO Strategic Communications Centre of Excellence, April 2020 (https://stratcomcoe.org/publications/download/analysis_of_sputnik_serbia_30-04_v4-1.pdf); Svetoka, S. and Doncheva, T., 'Russia's footprint in the Western Balkan information environment: susceptibility to Russian influence', NATO Strategic Communications Centre of Excellence, October 2021 (https://stratcomcoe.org/publications/download/Russias-footprint-in-the-Western-Balkan.pdf).

euiss

Published by the European Union Institute for Security Studies.
Printed in Luxembourg by the Publications Office of the European Union.

Cover image credit: Envato Elements

Publications Office of the European Union

PRINT ISBN 978-92-9462-199-3
CATALOGUE NUMBER QN-AK-23-018-EN-C
ISSN 2599-8943
DOI 10.2815/0253

PDF ISBN 978-92-9462-198-6
CATALOGUE NUMBER QN-AK-23-018-EN-N
ISSN 2315-1110
DOI 10.2815/869282