euiss European Union
Institute for Security Studies

RISING HYBRID THREATS IN AFRICA

BRIEF / 3
Mar 2022

Challenges and implications for the EU

The EUISS is an agency
of the European Union

CONFLICT
SERIES

by

Giovanni Faleg
Senior Analyst, EUISS

Nad'a Kovalčíková
Senior Analyst, EUISS*

Summary

- Hybrid threats in Africa have become a security concern for the EU. CSDP missions in the continent are increasingly the target of hybrid operations.
- Perpetrators of hybrid activities are state (e.g., Russia, China, Turkey) and non-state actors (e.g., Salafi-jihadist groups and private military contractors), operating in a growing list of African countries.
- Malign actors conduct hybrid operations to undermine the EU's capacity and credibility as a security provider, to hamper mission mandates and larger strategic interests, altering the relationship between the EU and African partners.
- Information manipulation is the most visible rising threat, alongside cyberattacks.
- Enhancing capacities to pre-empt and detect hybrid threats is vital to protect EU credibility and effective presence on the ground. There is a risk that some African countries may become operational hubs for growing hybrid activities, with a deteriorating impact on transnational security.

INTRODUCTION

Sub-Saharan Africa is becoming a testing ground for hybrid threats. While violent extremism and terrorism will remain security priorities for the continent in the next decade and beyond [1], hybrid operations are being increasingly detected. Today, multiple forms of hybrid threats constitute an exponential challenge in the transnational security landscape. The reason is threefold. First, the concept of hybrid threats is an 'umbrella concept' that regroups many different types of coercive and subversive activities, used by state or non-state actors to achieve specific objectives below the threshold of formally declared warfare [2]. These go beyond information manipulation and cyberattacks (often identified as common tools of foreign interference). They include support to violent non-state actors, use of private military contractors, targeting of critical infrastructure and foreign interference in elections. Malign actors frequently use these tools of interference in parallel, as part of a wider strategy. They serve as a catalyst for other actions and aim to exploit existing vulnerabilities while capitalising on confusion in the target state and a lack of adequate measures to address

The views expressed in this publication are solely those of the author(s) and do not necessarily reflect the views of the European Union.

them[3]. Second, state fragility and political instability in many African countries, combined with an aggravation of conflict and violence[4], provide a fertile ground for hybrid operations. Third, 'the new scramble for Africa'[5], defined as the increased geopolitical relevance of the African continent in a multipolar world[6], has created a battleground in which malign actors resort to hybrid tools such as cyberattacks and information manipulation (among which efforts to suppress credible and verifiable information), to gain influence or undermine the capacities and credibility of other powers, including the European Union.

However, the EU is not a passive witness to these developments. The Covid-19 pandemic has highlighted the need for intensified efforts and initiatives to protect the EU's presence[7] in the field from the harmful effects of hybrid threats[8]. Deployments under the Common Security and Defence Policy (CSDP) serve as a good indicator to assess to what extent the EU has become a direct target, and how broader European security interests can be affected by such threats. Missions have in fact been increasingly targeted by state and non-state actors conducting hybrid operations, as part of broader attempts to undermine the EU's credibility and interests in host countries, and by extension its role as a global security provider[9]. CSDP missions can be victims but also part of the solution. Through the deployment of these missions, the EU can contribute to countering hybrid threats and building resilience. These aspects (*protection from the threat* and *contribution to address the threat*) are at the heart of ongoing EU efforts to strengthen its tools to effectively counter hybrid threats and tactics.

Perpetrators of hybrid threats may not have the same interests or goals but all want to instrumentalise the EU on the ground.

This Brief seeks to explain why the EU should be alerted about the increase in hybrid threats in Africa and how they are becoming a critical security concern in an already fragile environment. First, it explains the nature of the threat to the EU's presence in Africa, providing examples of how CSDP missions are targeted by malign actors deploying hybrid threats. The second section identifies who these perpetrators are and what drives the expansion of hybrid threats in the continent. Finally, the third section discusses possible solutions, taking into account the lessons learnt from operational experience in CSDP missions, as well as the evolving fragility, conflict and violence trends in the region. It provides recommendations and policy options at the strategic level to enhance the resilience of host countries.

'BRUSSELS, WE HAVE A PROBLEM': AN ESCALATING THREAT TO THE EU IN AFRICA

There is mounting evidence that the evolving hybrid security landscape in Africa affects the EU's presence in the continent[10]. While many hybrid attacks go undetected, CSDP missions have reported several incidents in recent years, showing a similar pattern across different theatres and types of deployment. Hybrid operations targeting the EU encompass a wide range of malign tactics, which are often tailored and sequenced throughout a hybrid 'campaign' where initial activities serve to improve the chances of success of ensuing efforts. But campaigns can be more intense, coordinated or targeted, or take place later, to capitalise on confusion. Hybrid operations against the EU can also have a wide range of aims like harming a mission's reputation, sowing doubts within the local population, damaging local acceptance of EU presence, and discrediting reputation and credibility of the EU as well as of certain individuals. Such efforts may affect the morale and political rationale of an EU mission. Furthermore, perpetrators of hybrid threats may not have the same interests or goals but all want to instrumentalise the EU on the ground. Context inevitably has an impact on these aims. The level of threats to EU missions depends on whether they are targeted directly or perceived as an element of an overall Western endeavour.

Evidence of detected hybrid operations affecting CSDP missions can be found in the Central African Republic (CAR), Mali and Somalia, three difficult conflict-settings in which key EU security interests are at stake.

In CAR, the EU currently deploys a civilian advisory mission (EUAM) and a military training mission (EUTM)[11]. The political and economic situation in the country provides a relatively favourable environment for hybrid operations, including information manipulation activities. Russia has long recognised the strategic importance of Africa and continues to seize opportunities to extend its influence across the continent. To achieve its objectives in CAR, Russia does not hesitate to resort to hybrid tactics and pursue covert activities. In early 2018, several humanitarian convoys from Sudan entered CAR via Birao, officially to bring humanitarian aid (namely to install a field hospital in Bria). However, these convoys were generally composed of military vehicles carrying weapons and equipment. Russia also conducts information operations targeting the EU and its missions. Several articles in local newspapers portrayed the EU and its missions as poor partners in comparison to Russian trainers. In October 2020, the newspaper *L'Extension* published an article denouncing the mission EUTM RCA as a 'Machiavellian plan to weaken the Central African Armed Forces (FACA) with bad training'[12]. Numerous examples of such information manipulation have appeared in several newspapers in CAR, although their reach behind Bangui is limited. Distorted information is also widely reproduced through social media. The UN, France and the EU have been targeted by these campaigns to manipulate public opinion, through traditional media (mostly radio and newspapers), and through images, narratives and manipulated messaging online. Overall, the EUTM and EUAM do not seem to have been direct and systematic targets of information manipulation campaigns, as only one instance of such activity has been detected over a year ago. However, they can be affected collaterally when information manipulation activities focus on international organisations (EU, UN) or on individual Member States (as was the case with France[13]). When there is a lack of access to credible and authoritative news content and a Member State is a target of information manipulation, it becomes a concern for collective EU efforts.

In Mali, the EU has deployed a civilian capacity-building mission (EUCAP) and a military training mission (EUTM)[14]. While Mali has not been considered a hotbed for hybrid threats and the EU missions there were less affected than in CAR, it showcases a dangerous trend. First, there have been cases of Russia's involvement as a hybrid actor, confirmed by instances where opposition demonstrators held up pro-Russia signs ('*Vive la Russie!*') during election periods, asking Russia to be the saviour of Mali and criticising the West and France in particular. The private military company Wagner has also been increasingly present in Mali and their actions aimed at damaging the image of the EU have become frequent over time. Although EU deployments were not a direct target, these activities affect the way in which the missions are perceived locally and their ability to carry out their mandate. Recently, allegations that hybrid actors have been financing groups of opinion-makers and anti-systemic movements, threatening and possibly harming the EU and wider Western interests, have raised concerns[15]. In late 2019, anti-French messages and sentiment multiplied throughout Malian social media, rejecting France's presence in the region at a time when the G5 Sahel Summit in Pau was redefining international contributions to counter-terrorism efforts[16].

Although EU deployments were not a direct target, these activities affect the missions' ability to carry out their mandate.

In Somalia, the EU has deployed EUCAP *Nestor*, a civilian mission which assists host countries in developing self-sustaining capacity for enhancement of maritime security; and a military training mission (EUTM Somalia), which contributes to strengthening the Transitional Federal Government (TFG) and the institutions of Somalia[17]. A couple of incidents of information manipulation have been detected by the EU CSDP missions on social media, in particular Twitter, intended to portray the EU in a negative light. In combination with other local challenges such as detection and protection from improvised explosive devices, the EU mission needed to increase awareness raising efforts and trainings to detect and respond to evolving threats in an adequate and timely manner, putting additional pressure on their core mandate.

The implications of these activities for the EU can be threefold. First, at the strategic level, hybrid threats can severely undermine the EU's credibility as a trustworthy and honest provider of security, an economic partner or diplomatic actor. Second, at the operational level, they can hamper mission mandates, specific tasks, the implementation of projects and jeopardise outcomes to the detriment of CSDP engagements. Third, hybrid threats can destabilise the security situation in the host state, which may produce a direct threat to the EU's presence on the ground (for instance, the physical safety of EU staff), but also affect larger EU economic and political interests, for instance if the relationship between the EU and the host government is altered by changing perceptions due to information manipulation. Moreover, the relationship between the EU and its host country may also affect how successful EU strategies to counter hybrid threat are.

WHAT'S IN A NAME? IDENTIFYING AND DETECTING HYBRID THREATS

Having assessed the nature of the hybrid threat posed to the EU in Africa, let us now turn to its drivers, forms and perpetrators. To begin with the drivers, the emergence of a hybrid landscape in Africa relates to megatrends such as climate change and the demographic boom. These create challenges to sustain the needs of a growing population while mitigating environmental degradation. Other factors are technological progress and digital transformation, characterised

HYBRID AHEAD

An escalating threat to the EU in Africa

Hybrid threats are scaling up in sub-Saharan Africa. Especially in areas affected by fragility, conflict and violent extremism. This can lead to a spill-over, compromising both African and European security.

Fragility

■ High institutional and social fragility

■ Medium intensity conflict

■ High intensity conflict

CSDP

Civilian mission

△ Personnel

◌ Budget (€ million)

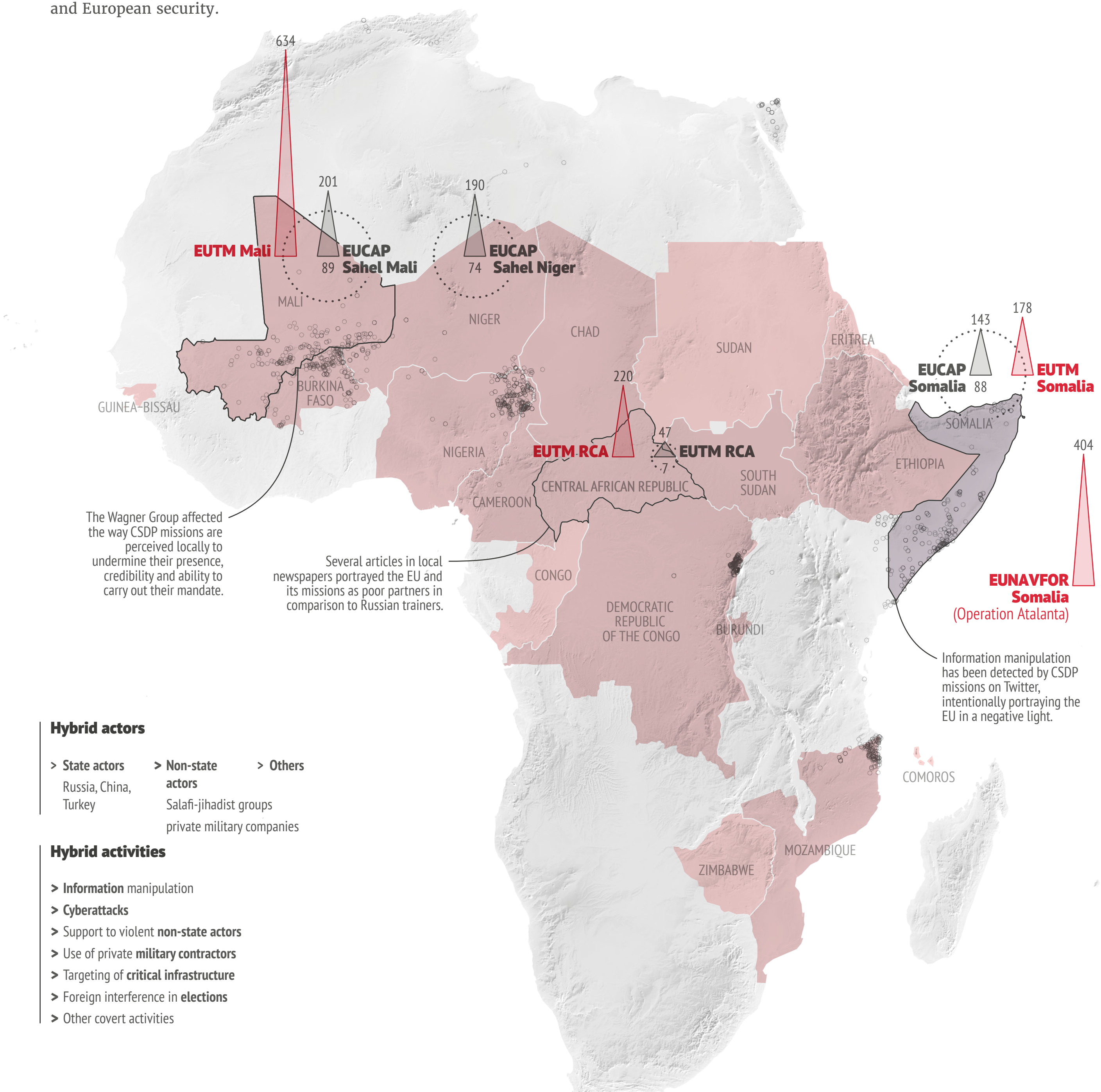
Military operation

△ Personnel

Jihadist violence

2021

○ One circle = one event



The Wagner Group affected the way CSDP missions are perceived locally to undermine their presence, credibility and ability to carry out their mandate.

Several articles in local newspapers portrayed the EU and its missions as poor partners in comparison to Russian trainers.

Information manipulation has been detected by CSDP missions on Twitter, intentionally portraying the EU in a negative light.

Hybrid actors

> **State actors**
Russia, China, Turkey

> **Non-state actors**
Salafi-jihadist groups
private military companies

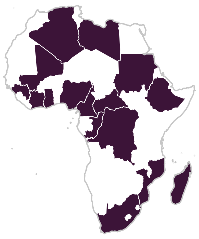
> **Others**

Hybrid activities

> **Information** manipulation
> **Cyberattacks**
> Support to violent **non-state actors**
> Use of private **military contractors**
> Targeting of **critical infrastructure**
> Foreign interference in **elections**
> Other covert activities

Influence

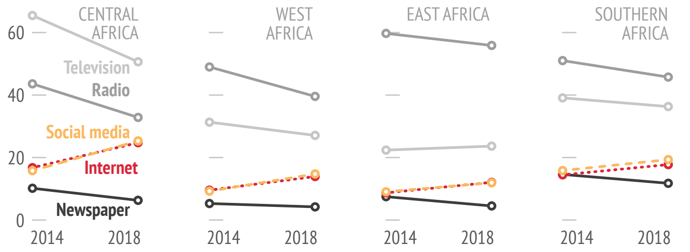
Russia engages in information manipulation in these countries.



Sources of daily news

Change in regional average, 2014–2018

In a changing African media landscape, hybrid actors can effectively use different information channels to manipulate media messaging.



Data: European Commission, GISCO, 2022; EEAS, 2022;
UCDP, Georeferenced Event Dataset (GED) Global version 21.1, 2021;
Afrobarometer, 2019; IMF, 2022; EUISS, 'Yearbook of European Security', 2021

for instance by a growing number of internet and social media users, and enhanced connectivity[18].

Hybrid actors tend to target and exploit situations where fragility, conflict and violence are expanding. They capitalise on the inability of African governments to provide effective governance and service delivery (housing, education, health, water and sanitation), including the provision of security in ungoverned or contested spaces. For instance, in Somalia, the jihadist group al-Shabaab circulated false claims about the safety of healthcare facilities, discouraging Covid patients from getting treated there, to undermine the country's government and stability[19]. Similarly, jihadist propaganda efforts in the Sahel often depict international and particularly Western governmental and non-governmental organisations through imperialist lenses, to increase scepticism and mistrust towards them.

The use of hybrid tools, tactics and strategies applied in one place, affects also other geographical areas and societal domains.

Systemic factors also play a role. Africa is becoming a hybrid battleground in a broader geopolitical confrontation among powers attempting to disrupt each other's strategic objectives, such as investments in critical infrastructure, civilian and military presence, human rights and democracy promotion, access to natural resources and trade. This creates additional pressure on African states' capacities, both from state and non-state actors. Russia's information manipulation activities have targeted various African nations, including Algeria, Cameroon, CAR, the Republic of the Congo, Côte d'Ivoire, the Democratic Republic of the Congo (DRC), Ethiopia, Ghana, Guinea, Libya, Madagascar, Mali, Mozambique, Nigeria, South Africa and Sudan[20]. The clearest example of Russian information manipulation targeting Africa was uncovered by Facebook in October 2019. Facebook took down dozens of inauthentic coordinated accounts linked to Russian oligarch Yevgeny Prigozhin, who was seeking to spread distorted messages and promote Russian interests in eight African countries[21]. The content, which was published by fabricated profiles and accounts of subcontracted locals, criticised 'Western imperialism' and supported allied rulers (e.g. President Omar al-Bashir of Sudan or President Alpha Condé of Guinea), while reinforcing the idea that Russia wants to be Africa's equal partner. Such activities can be easily replicated.

Africa is becoming a hybrid battleground in a broader geopolitical confrontation among powers.

For the reasons outlined above, Sub-Saharan Africa provides fertile territory for malign actors to set up hybrid operations and test old tactics and tools in new settings or contexts, particularly if this can contribute to gain control of spaces that have become more 'valuable' from a geopolitical and geo-economic standpoint because they provide an economic, political, technological or military advantage. Yet, which forms of hybrid threats have been more prominent in Africa so far, based on observable events?

First of all, early detection of hybrid threats is difficult due to their cross-cutting character and spill-over effects. The use of hybrid tools, tactics and strategies applied in one place, affects also other geographical areas and societal domains. This spill-over effect, characterised by an impact beyond the direct targets, demonstrates how hybrid actors exploit the interconnectedness of their targets, especially in the cyberspace and public spheres. For instance, news articles about the EU or a specific EU Member State published in African media will likely also reach European audiences and beyond, which may lead to doubts, breakdown of trust or negative perceptions not only in Africa. This may further worsen diplomatic relations, contribute to societal tensions or increase the influence of seemingly independent third actors. As malign actors tend to conduct hybrid attacks in parallel and combine various tools, it makes them more difficult to detect, address or even prevent effectively, as the context of their use and the deployment of the tactics may become clearer only at a later stage. One solution is to systematically monitor and identify hybrid activities in other regions[22]. Hybrid actors tend to replicate and nuance their existing tools and tactics, building on their experience in other regions and tailoring them to new targets, while further undermining transnational security.

On that account, the most prominent rising form of hybrid threat in the continent is information manipulation, an intentional and often covert use of media, manipulating public discourse to mislead and cause harm. It encompasses 'three criteria: a coordinated campaign, the diffusion of false information or information that is consciously distorted [or intentional suppression of information], and the political intention to cause harm' [23]. In contexts characterised by competing narratives, information manipulation can be used to influence perceptions on the ground in a convenient manner or fuel a conflict by creating confusion. In Ethiopia for instance, both the national and international community raised concerns about the active contribution of information manipulation and hate speech in the escalation of the civil war. The proliferation of such disruptive and divisive efforts in the country is an issue that social media companies continue to fail to address. In addition, the Ethiopian government blocked citizens' access to the international press, leading to an information vacuum in which such manipulative activities tend to thrive[24].

Moreover, sub-Saharan Africa continues to be the region with the greatest gap in internet coverage and usage, with more than a half of the population not using mobile internet[25]. While not representing the average rise in online media usage in Sub-Saharan Africa, CAR is a noteworthy example with its growing, yet still very low, access to the internet (over 11 % of internet users)[26] and even lower numbers of active social media users (2.9 %)[27], with radio being the national media with the highest audience[28]. Yet, as access to diversified and credible information remains limited, hybrid actors can trigger public opinion in a relatively easy and cheap way. However, what the data also shows is the need to understand and approach the Sub-Saharan Africa region in a nuanced way. While growing internet coverage and usage increases the potential for digital hybrid activities, the significant differences in such connectivity between individual countries, also influences the access to diverse and verifiable information.

Finally, a number of foreign powers are known to have vested interests and presence in the region prompting them to resort to hybrid activities, taking advantage of the African states' low capacities and lack of resilience to hybrid threats[29]. In addition to Russia[30], whose engagements are widely debated in the think tank, policy and most prominently in the intelligence community, China and Turkey also use information operations to project their influence in Africa, introducing uncertainty around official narratives for political gains. China has used information manipulation to push back against claims of genocide and human rights abuse in Xinjiang[31], to challenge narratives on the coronavirus[32] and to defend its image and feed anti-Western rhetoric. Turkey has significantly expanded its hard and soft power in the past few years[33]. It has also strengthened its penetration in African media. In addition, education, and notably the establishment of Turkish schools, has enabled Turkey to project its national interest, history, language and culture in Africa. While these engagements do not constitute a hybrid threat *per se*, they have been raising concerns among EU Member States as they provide a capacity and a large infrastructure to potentially distort information against the West and Western international organisations.

Hybrid threats in Africa also come from non-state actors, specifically Salafi-jihadist groups.

Hybrid threats in Africa also come from non-state actors, specifically Salafi-jihadist groups. Whether the Islamic State in the Sahara-Sahel, al-Shabaab in Somalia or Boko Haram in Nigeria, groups exploit disputes between ethnic groups and use these to boost recruitment or consolidate their local standing. These groups operate in the public spheres and increasingly in urban centres, by building on anti-colonialism narratives and by presenting themselves as local actors expelling foreign forces[34].

To conclude, a number of state and non-state malign actors target a long list of African countries. Observable evidence points to information manipulation as the most visible growing threat that has emerged in the continent, enhancing the overall impact of hybrid activities. However, existing tools to detect hybrid operations in the region lack consistent and comparable data, more systematic intelligence collection, and suitable information sharing mechanisms, which hampers a more comprehensive analysis of the threat.

WHAT CAN BE DONE? LESSONS AND POLICY OPTIONS

The operational experience with CSDP missions in sub-Saharan Africa has already allowed EU policy planners to identify a number of lessons, particularly in three areas: situational awareness, strategic communication and resilience building.

First, the level and types of hybrid threats targeting the EU in the field depend on contextual factors, such as a poor socio-economic context in the host country or local grievances. Hybrid activities can increase if the mission's mandate and operational territory overlaps with areas where hybrid actors have stakes. This can be relevant for CSDP missions contributing to preventing or countering violent extremism in the Sahel, Somalia and Mozambique. Other factors affecting the impact of hybrid threats include disruptive events such as a regime change or uprisings. These can make it easier for hybrid actors to carry out attacks, like in Mali. Moreover, EU missions are more susceptible to attacks if the EU presence is perceived as an element of a Member State's post-colonial policy or part of a broader Western effort. All this makes it necessary for the EU to develop a common situational awareness in order to understand the driving forces behind hybrid attacks in a specific theatre, and better prepare and implement deterrence and prevention measures.

Second, an effective strategic approach by the EU would need to conceive and plan civilian CSDP missions as elements of a broader strategic communication[35] approach, and not the other way around (strategic communication as one component of civilian CSDP missions). EU deployments have capability shortfalls in this area, which hampers both proactive and reactive crisis communication during an incident or tailored communication with the local audience, especially in times of crisis. Highlighting the objectives and values of missions and the tangible results and benefits of EU action could be a powerful instrument, as fact-based information is recognised as an effective way to counter information manipulation. What also matters is that information reaches all levels, from CSDP missions and EU delegations (field) to political leadership and EU Member States.

Third, if requested by the host country, EU actors can assist local governments with work on legislation adaptation, provide advice to select intelligence services, and offer training in various areas such as capacity building and raising awareness with local partners. Ultimately, however, the commitment of the host state's central authorities to the EU strategy to combat information manipulation campaigns is fundamental to resist and/or even stop these hybrid campaigns. Short of a sustained political dialogue with the host state's authorities, undesired outcomes like state failure, complex transition processes, protracted conflicts or relapses into authoritarian regimes may complicate the EU's ability to deliver effective capacity building.

Building on the lessons above, better capacity to pre-empt and detect hybrid threats is a salient starting point and a critical issue for the EU to focus on. Investment in the following enablers could enhance such capacity:

- **Intelligence**: a common and centralised EU situational awareness approach across EU institutions towards hybrid threats in specific fields of operation.
- **Early warning**: a dedicated mechanism to facilitate early detection of hybrid threats in close contact with CSDP missions.
- **Partnerships**: information sharing with allies and regional partners, particularly the African Union, to systematically monitor malign actors' activities and behaviour.
- **Technology**: use of artificial intelligence to help CSDP missions to better analyse and assess their operational environment through social media.
- **Human factor**: enhanced training for mission staff to understand how hybrid actors may exploit the consequences of their individual or collective actions and responses.

The security threat that information manipulation in the African continent can pose to the European infosphere is reminiscent of the threat intermediate-range nuclear missiles posed to Europe's territorial defence during the Cold War. 'Infomissiles'[36] are rapidly scaling up in sub-Saharan Africa. Enhancing capacities to pre-empt and detect them is becoming all the more vital to protect EU credibility and presence on the ground, and enable the Union to adequately assist partner countries. Failure to do so could result in some African countries becoming operational hubs for growing hybrid activities.

References

[*] The authors would like to thank Nuria Portero and Ricardo Farinha for their dedicated research assistance.

[1] Faleg, G. and Mustasilta K., 'Salafi-jihadism in Africa: a winning strategy', *Brief* No 12, EUISS, June 2021 (https://www.iss.europa.eu/content/salafi-jihadism-africa).

[2] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication - Joint Framework on countering hybrid threats: a European Union response', JOIN(2016) 18 final, 6 April 2016, p. 2 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN).

[3] Berzina, K., Kovalčíková, N., Salvo, D. and Soula E., 'European Policy Blueprint for Countering Authoritarian Interference in Democracies', ASD, GMF, 2019 (https://www.gmfus.org/news/european-policy-blueprint-countering-authoritarian-interference-democracies).

[4] The year 2019 saw the highest number of state-based conflicts in the African continent since 1946, while non-state armed conflicts have also proliferated in the past decade. These trends have worsened during the Covid-19 pandemic. 2021 has seen an unexpected rise in insurrections and unconstitutional changes of government due to military takeovers, especially in West Africa (Chad, Mali and Guinea). For a fuller picture, see: Mustasilta, K., 'From bad to worse? The impact(s) of Covid-19 on conflict dynamics', *Brief* No 13, Conflict Series, EUISS, June 2020 (https://www.iss.europa.eu/content/bad-worse-impacts-covid-19-conflict-dynamics); Mustasilta, K., 'Conflict trends', in Faleg, G. (ed), 'African Futures 2030: free trade, peace and prosperity', *Chaillot Paper* No 164, EUISS, February 2021, pp. 28-31 (https://www.iss.europa.eu/content/african-futures-2030).

[5] 'The new scramble for Africa', The Economist, 9 March 2019 (https://www.economist.com/leaders/2019/03/07/the-new-scramble-for-africa).

[6] Faleg, G. and Palleschi, C., 'African Strategies: European and global approaches towards sub-Saharan Africa', *Chaillot Paper* No 158, EUISS, June 2020 (https://www.iss.europa.eu/content/african-strategies).

[7] The authors of this Brief have chosen to narrow down the focus on CSDP deployments as the EU's 'forward presence' in the field, hence leaving aside EU and Member States delegations, and other forms of presence and engagement that may be affected by hybrid threats. The Brief in particular, looks at civilian CSDP missions.

[8] Council of the European Union, 'Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic', 15 December 2020, p. 2 (https://data.consilium.europa.eu/doc/document/ST-14064-2020-INIT/en/pdf).

[9] As highlighted by a recent debate organised by the European Parliament Security and Defence Subcommittee, on the impact of disinformation campaigns against the EU military and civilian missions and operations (https://www.europarl.europa.eu/news/en/press-room/20201115IPR91702/csdp-disinformation-targeting-eu-missions-and-operations).

[10] The evidence collected here is the result of first-hand fieldwork research by the authors, conducted during the autumn of 2021.

[11] The objective of EUTM is to support the build-up of a modernised, effective, credible, ethnically balanced and democratically accountable Central African Armed Forces (FACA). The objective of EUAM is to provide strategic advice to the CAR Ministry of Interior and Public Security and to the Internal Security Forces. Both operate in the framework of the EU's integrated approach to conflicts and crises. Source: EEAS website, EUAM CAR and EUTM CAR missions factsheets, October 2021.

[12] Source: EUTM RCA.

[13] See: RFI, 'France accuses CAR of complicity in disinformation campaign, suspends support', 8 June 2021 (https://www.rfi.fr/en/africa/20210608-france-accuses-car-of-complicity-in-disinformation-campaign-suspends-support-russia-wagner-mercenaries-social-media-politics-protests).

[14] The objective of EUCAP Sahel Mali is to support Mali's internal security forces and civilian administration to strengthen good governance and the rule of law. The objective of EUTM is to deliver advice to the Ministry of Defence and the Malian Armed Forces (MaAF), including military education and training to support the Malian authorities to reach a self-sustainable MaAF able to contribute to the defence of the Malian territory and to the protection of the Malian population. Both operate under the umbrella of the EU's integrated approach to conflicts and crises, and in close cooperation with EUCAP Sahel Niger and EUBAM Libya. Source: EEAS website, EUCAP Sahel Mali and EUTM Mali missions factsheets, October 2021.

[15] See, for instance: Sangare B. and Diallo, F., 'Russia-Mali: who is spreading Moscow's soft power in Bamako?' The Africa Report, 25 November 2021 (https://www.theafricareport.com/150126/russia-mali-who-is-spreading-moscows-soft-power-in-bamako/).

[16] Philippe Chapleau, 'Au Sahel, les fake news se multiplient sur fond de rejet de la présence française', Ouest France, 16 December 2019 (https://www.ouest-france.fr/monde/mali/au-sahel-les-fake-news-se-multiplient-sur-fond-de-rejet-de-la-presence-francaise-6656726).

[17] EEAS website, EUCAP Nestor and EUTM Somalia missions factsheets, November 2021.

[18] Van Raemdonck, N., 'Africa as a cyber player', *Digital Dialogue Report*, EU Cyber Direct, January 2021 (https://eucyberdirect.eu/research/africa-as-a-cyber-player).

[19] NATO Centre of Excellence Defense Against Terrorism, 'Study on Africa: A hybrid battleground', 2020 (https://www.tmmm.tsk.tr/publication/reports/COE_DAT_study_on_Africa_a_hybrid_battleground_14082020.pdf).

[20] 'Russian Disinformation in an African Context', *IntelBrief*, The Soufan Center, 2019 (https://thesoufancenter.org/intelbrief-russian-disinformation-in-an-african-context/).

[21] France24, 'Russian disinformation campaign targeted Africa: Facebook', 30 October 2019 (https://www.france24.com/en/20191030-russian-disinformation-campaign-targeted-africa-facebook).

[22] Kovalčíková N., 'What if ... the Western Balkans turn away from the EU?', in Gaub, G. (ed) 'What if ... not? The cost of assumptions', *Chaillot Paper* No 172, EUISS, January 2022, pp. 58-62 (https://www.iss.europa.eu/content/what-ifnot-cost-assumptions).

[23] Jeangène Vilmer, J-B., Escorcia, A., Guillame, M. and Herrera J., 'Information Manipulation, A Challenge for Our Democracies', Policy Planning Staff (CAPS, Ministry for Europe and Foreign Affairs) and the Institute for Strategic Research (IRSEM, Ministry for the Armed Forces), August 2018, p. 21 (https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf).

[24] Wilmot, C., Tveteraas, E. and Drew, A., 'Dueling Information Campaigns: The War Over The Narrative in Tigray', The Media Manipulation Casebook, August 2021 (https://mediamanipulation.org/case-studies/dueling-information-campaigns-war-over-narrative-tigray).

[25] GSMA, 'The state of mobile internet connectivity in Sub-Saharan Africa: why addressing the barriers to mobile internet use matters now more than ever', October 2021 (https://www.gsma.com/mobilefordevelopment/blog/the-state-of-mobile-internet-connectivity-in-sub-saharan-africa/).

[26] Datareportal, 'Digital 2021: the Central African Republic' (https://datareportal.com/reports/digital-2021-central-african-republic) p. 17.

[27] Ibid.

[28] Media Landscapes, Central African Republic (https://medialandscapes.org/country/central-african-republic).

[29] 'Study on Africa: A hybrid battleground', op. cit.

[30] Faleg, G. and Secrieru, S., 'Russia's forays into sub-Saharan Africa: do you want to be my friend, again?' *Brief* No 6, EUISS, March 2020 (https://www.iss.europa.eu/content/russias-forays-sub-saharan-africa).

[31] SupChina, 'Why are Chinese officials in Africa so active in messaging on Xinjiang?', 3 February 2021 (https://supchina.com/2021/02/03/why-are-chinese-officials-in-africa-so-active-in-messaging-on-xinjiang/); Essa, A., 'China Is Buying African Media's Silence', *Foreign Policy*, 14 September 2018 (https://foreignpolicy.com/2018/09/14/china-is-buying-african-medias-silence/).

[32] Cook, S., 'Beijing's Coronavirus Propaganda Has Both Foreign and Domestic Targets', Perspectives, Freedom House, 20 April 2020 (https://freedomhouse.org/article/beijings-coronavirus-propaganda-has-both-foreign-and-domestic-targets); Madrid-Morales, D., Börekci, D., Löffler, D. and Birkevich, A., 'It is about their story: How China, Turkey and Russia influence the media in Africa', Konrad-Adenauer-Stiftung, Regional Media Programme Sub-Sahara Africa, January 2021 (https://www.kas.de/en/web/medien-afrika/einzeltitel/detail/-/content/it-is-about-their-story).

[33] For details about Turkish soft/hard power engagement in sub-Saharan Africa, see: 'African Strategies: European and global approaches towards sub-Saharan Africa', op.cit., pp. 69-72. Also: Gbadamosi, N., 'Turkey deepens its footprint in Africa', Foreign Policy, 22 December 2021 (https://foreignpolicy.com/2021/12/22/turkey-africa-erdogan-partnership-summit/).

[34] 'Salafi-jihadism in Africa: a winning strategy', p. 5, op. cit.

[35] European Parliamentary Research Service, 'Strategic communications as a key factor in countering hybrid threats', March 2021 (https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)656323).

[36] Term inspired by the 'Euromissiles crisis', to describe security consequences for Europe of hybrid threats proliferating in Africa.

euiss

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

Cover image credit: EUCAP Sahel Mali/flickr

Publications Office
of the European Union

PRINT ISBN 978-92-9462-088-0
CATALOGUE NUMBER QN-AK-22-003-EN-C
ISSN 2599-8943
DOI 10.2815/806028

ONLINE ISBN 978-92-9462-087-3
CATALOGUE NUMBER QN-AK-22-003-EN-N
ISSN 2315-1110
DOI 10.2815/120212