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, 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. 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 these challenges.
them. Second, state fragility and political instability in many African countries, combined with an aggravation of conflict and violence, provide a fertile ground for hybrid operations. Third, ‘the new scramble for Africa’, defined as the increased geopolitical relevance of the African continent in a multipolar world, 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 in the field from the harmful effects of hybrid threats. 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. 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.

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.

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

‘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. 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). 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...
In Mali, the EU has deployed a civilian capacity-building mission (EUCAP) and a military training mission (EUTM). While Mali has not been considered a hotspot 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 missions' ability to carry out their mandate.

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
- Military operation
  - Budget (€ million)

**Jihadist violence**
- 2021
  - One circle = one event

**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.

**EUCAP**
- Somalia
- Sahel Niger
- Sahel Mali

**EUTM RCA**
- Somalia
- Burundi
- Cameroun
- Congo
- South Sudan
- Chad
- Sudan

**EUTM Mali**
- Malian

**EUNAVFOR**
- Somalia (Operation Atalanta)

**Sources of daily news**

- Internet
- Newspaper
- Radio
- Social media
- Television

**Change in regional average, 2014−2018**

- Central Africa
- West Africa
- East Africa
- Southern Africa

for instance by a growing number of internet and social media users, and enhanced connectivity\(^\text{an}\).

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\(^\text{am}\).

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.

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\(^\text{an}\). 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\(^\text{am}\).

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.

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\(^\text{a}\).

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\(^\text{am}\). 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

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

Africa is becoming a hybrid battleground in a broader geopolitical confrontation among powers.
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\(^{(26)}\).

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\(^{(29)}\). 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)\(^{(31)}\) and even lower numbers of active social media users (2.9\%)\(^{(27)}\), with radio being the national media with the highest audience\(^{(31)}\). 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\(^{(28)}\). 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\(^{(30)}\), to challenge narratives on the coronavirus\(^{(30)}\) and to defend its image and feed anti-Western rhetoric. Turkey has significantly expanded its hard and soft power in the past few years\(^{(31)}\). 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 \textit{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. 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 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’ 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.
- 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.
- The evidence collected here is the result of first-hand fieldwork research by the authors, conducted during the autumn of 2021.
- The objective of EUTM is to support the build-up of a modernised, effective, credible, ethically 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.
- Source: EUTM RCA.

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 EUM 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 EUM Mali missions factsheets, October 2021.


EEAS website, EUCAP Nestor and EUM Somalia missions factsheets, November 2021.


Ibid.


‘Study on Africa: A hybrid battleground’, op. cit.

Faleg, G. and Secirié, S., ‘Russia’s forays into sub-Saharan Africa: do you want to be my friend, again?’, Brief No 6, EUIS, March 2020 (https://www.eu.is.europa.eu/content/russias-forays-sub-saharan-africa).


‘Term inspired by the ‘Euromissiles crisis’, to describe security consequences for Europe of hybrid threats proliferating in Africa.


(19) www.iss.europa.eu/content/russias-forays-sub-saharan-africa you want to be my friend, again?’.