zif Center for International Peace Operations

100 Voices on Technology & Peace Operations

Managing cyber security in peace operations

A policy response to foreign information manipulation's impact on civilian CSDP missions

11 July 2022 | Crista Huisman

Hybrid threats are an increasingly complex security challenge for the EU, also affecting its civilian Common Security and Defence Policy (CSDP) missions. Malign actors target the EU at large and aim to derail EU's global engagement. One hybrid modus operandi that affects our civilian missions is information manipulation. This form of malign influencing both targets the EU's objectives and interests as a whole, and is aimed at undermining the EU missions' operational effectiveness and reputation. The risks of information manipulation and interference for civilian CSDP, as one form of hybrid threats, are recognised in the Civilian CSDP Compact. The Strategic Compass places even more emphasis on the topic.

In this article, basing myself on these two documents (Strategic Compass and Civilian CSDP Compact), I will briefly elaborate on current initiatives to tackle the risks of information manipulation. I will focus in particular on initiatives to tackle hybrid threats (notably the EU hybrid toolbox, the EU hybrid rapid response teams), the Foreign Information Manipulation and Interference (FIMI) toolbox and work ongoing specifically on civilian CSDP, guided by the mini-concept on hybrid threats.

STRATEGIC COMPASS: EU HYBRID TOOLBOX AND EU HYBRID RAPID RESPONSE TEAMS

Russia's unprovoked and unjustified attack on Ukraine signifies a tectonic shift in the European security and defence architecture. It demonstrates once again the need for a comprehensive response - military support measures and civilian crisis management, the latter covering the information space as a new domain. We are witnessing that a wide range of hybrid actions can take place both before military aggression – for priming purposes – and in combination with it. For example, cyber-attacks on public services of Ukraine, attacks on online infrastructure or the rerouting of internet access from occupied areas through the Russian internet.

100 Voices on Technology & Peace Operations

The Strategic Compass highlights how hybrid actors are constantly refining and strengthening their tactics, techniques and procedures. We saw an example of this last year when the EU faced a hybrid attack involving the instrumentalisation of migration. To respond to this challenge, the Compass proposes that a wide range of existing and possible new EU tools be brought together within a broader EU hybrid toolbox. The toolbox should comprise preventive, cooperative, stabilisation, restrictive and recovery measures, as well as strengthen solidarity and mutual assistance. Working on this toolbox, the Council has recently agreed conclusions on a framework for a coordinated response to hybrid campaigns affecting the EU and its Member States. Within this overall framework, the hybrid toolbox could act in a coordinated manner with other relevant sectoral mechanisms, such as the cyber diplomacy toolbox and the forthcoming EU toolbox to counter what the EU terms Foreign Information Manipulation and Interference (FIMI).

The Strategic Compass also expresses the intention to create EU Hybrid Rapid Response Teams, as part of the hybrid toolbox. While the concept and scope is still in the design phase, the idea is that these would be small advisory teams whose shape and composition would depend on the needs of each individual case. These teams should be adaptable to the threat and draw on relevant sectoral national and EU civilian and military expertise to support Member States, CSDP missions and operations, as well as partner countries in countering hybrid threats.

FOREIGN INFORMATION MANIPULATION AND CIVILIAN CSDP MISSIONS

Information manipulation is an increasingly important challenge for our CSDP missions in the field. Recent events and developments have shown, particularly across the African continent but also elsewhere, how foreign actors often use foreign information manipulation and interference as one part of the wider hybrid threats spectrum to target the EU, its Member States and its strategic partners. Missions strategic footprints in a region or a geographical area are systematically eroded by foreign information manipulation and interference, and more importantly, their space for pro-active, strategic communication is steadily shrinking. In some of the local, volatile information environments of the missions, where access to reliable information is scarce and influence is highly (but not exclusively) driven by social media content, it became easier for foreign actors to advance their influence and control the information environments of target audiences. In many cases, despite the apparent focus and centre of gravity outside the EU, the effects of their hybrid campaigns often occur also at EU level – seeking to interfere with or undermine our internal decision-making processes as well as our common foreign policy priorities, embedded in the CSDP mandates.

From this complex perspective, the EU has to address a constantly evolving challenge, which has the potential to transform the local information environments into hostile environments and ultimately poses a threat to our foreign and security policy. To this end, the EU's revamped approach to counter foreign information manipulation put forward by the Strategic Compass, represents an ambitious milestone towards a more resilient EU as well as for an effective response to such threats.

100 Voices on Technology & Peace Operations

CIVILIAN CSDP COMPACT AND THE MINI-CONCEPT ON HYBRID THREATS

Hybrid threats were highlighted in the Civilian CSDP Compact as one of the focus areas for civilian CSDP. To support Member States and EU services in identifying potential areas of increased efforts in this field, my sector has drafted a so-called mini-concept on hybrid threats. The aim of the mini-concept is to explore what civilian missions could do in the area of hybrid threats, how this links with other actors on the ground, and which capabilities would be needed to realise this on the ground. The mini-concept on hybrid threats focuses on two aspects: (1) what a CSDP mission can do to strengthen the EU's and its own resilience, and (2) CSDP support to host state authorities.

As far as the mission's own resilience is concerned, all mission personnel need to be properly trained, including concerning the general awareness of hybrid threats. A "whole-of-mission" approach has to be put in place to protect the mission against potential threats. In addition, hybrid threats to the mission or the host state need to be properly identified and analysed. It is of crucial importance to ensure that such analysis is shared with other EU institutions to contribute to the overall situational awareness, including hybrid threats and information manipulation in missions' theatres.

The strengthening of the host state's resilience to hybrid threats can be achieved through various means, primarily through capacity building. Support to the host state's strategic communication and analytical capacities can be examples. Member States can also decide to include specific lines of operations into the mission's mandate concerning hybrid threats. Furthermore, as a follow-up of the Hybrid Risk Survey, if completed in the given host nation, CSDP missions could provide support to the host state through the development of national strategies and legislation, as well as through advice, capacity building and potentially (if the mandate permits) training for dedicated host state authorities and specialised units.

The mini-concept is a first step to reinforce civilian CSDP actions further in the field of countering hybrid threats. Other steps need to follow. In taking them, civilian CSDP missions need to be joined up with other initiatives, such as the hybrid toolbox and the Hybrid Rapid Response Teams mentioned earlier.

To be effective and efficient, sufficient capabilities are needed to ensure that civilian CSDP missions can contribute to the overall EU effort to counter hybrid threats and address foreign information manipulation. The EU and its Member States will need to build capabilities in various fields, but foremost analytical, cybersecurity and strategic communication skills. Tailor-made training needs to be developed and synergies with other initiatives made.

100 Voices on Technology & Peace Operations

CONCLUSION

Information manipulation, as part of increasingly sophisticated hybrid threats, is challenging the EU and its civilian CSDP missions. The response to it cannot be simply reduced to 'better' strategic communication. It has to be tackled in a comprehensive manner using all tools and initiatives, such as the EU hybrid toolbox, EU Hybrid Rapid Response Teams, the forthcoming FIMI toolbox and the mini-concept on hybrid threats. These efforts will form part of a bigger response to the challenges related to information manipulation and its effect on the strategic and operational theatre.

ABOUT THE AUTHOR

Crista Huisman is the Head of Sector for Civilian Crisis Management (CSDP) in the EEAS. In this position she is responsible for the policy development of the EU's civilian missions, including the coordination and implementation of the Civilian CSDP Compact. Her work includes strengthening the internal-external security nexus (cooperation with Justice and Home Affairs actors such as Europol, Frontex and Eurojust) and Civilian Capability Development. Previously, Crista has worked as a senior officer in various assignments within the CSDP missions in Ukraine and Georgia. She currently resides with her husband and two daughters in Brussels. She can be reached under crista.huisman@eeas.europa.eu.