



DECEMBER 2022

## Realising the EU Hybrid Toolbox: opportunities and pitfalls

In recent years European and other nations have been increasingly targeted by different manipulation or coercion tactics that remain under the threshold of violence, and are commonly referred to as hybrid threats.<sup>1</sup> For instance, in 2016 the elections in the United States were manipulated by a foreign state actor through targeted propaganda and the leaking of hacked material that compromised one of the presidential candidates. In the same year the British referendum on remaining in the European Union was also targeted by sophisticated propaganda efforts.<sup>2</sup> The need to counter these threats and deal with them comprehensively has therefore been acknowledged in the EU Strategic Compass. It provides for the development of a toolbox to put at the disposal of member states a wide range of measures to respond to hybrid campaigns, should they choose to invoke the assistance of the EU. This EU Hybrid Toolbox (EUHT) intends to gather all civilian and military instruments that can be employed to counter hybrid campaigns. Operationalisation was intended by the end of 2022 but this no longer seems attainable. However, the conflict in Ukraine has demonstrated the importance of having a coordinated reaction capability to counter hybrid campaigns and is likely to provide the momentum to bring the development of the EUHT to fruition.

This policy brief examines the most recent progress on operationalising the EUHT. First, the rationale for the EUHT is explained. Next, the state of play in the operationalization process is analysed. The subsequent section focusses on the difficulties stemming from differences of opinion between the member states, followed by an assessment of the issues surrounding decision-making. After suggestions for increasing the effectiveness of the EUHT are given, the policy brief ends with conclusions and a listing of opportunities and pitfalls.<sup>3</sup>

- 1 For the debate on defining hybrid threats, see Dick Zandee, Sico van der Meer and Adája Stoetman, [Countering hybrid threats: steps for improving EU-NATO cooperation](#), Clingendael Report, October 2021, p. 2-5; Georgios Giannopoulos, Hanna Smith and Marianthi Theocharidou, [The landscape of Hybrid Threats: A conceptual model](#), Publications Office of the European Union, February 2021.
- 2 United States Senate, [Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security](#), Committee on Foreign Relations, 115<sup>th</sup> Congress, 2018, p. 116-118.
- 3 The methodology used for this policy brief consists of a combination of literature scanning and a limited number of interviews. The author would like to thank the interviewees for their valuable input that was given under the application of the Chatham House Rule.

## Why these measures?

What is currently called hybrid threats is not exactly a new phenomenon. In fact, deniably manipulating affairs in other countries by “discreet forms of intervention that obviated more violent methods”<sup>4</sup> has been part and parcel of international statecraft for centuries. Other terms in use are ‘alternative means,’ ‘the quiet option,’ ‘covert action,’ or ‘active measures’ (*aktivnye meropriyatiya*). The tactics involved are a mixture of legal and illegal, conventional and unconventional means, including clandestine foreign interference in political processes (elections and policy), offensive cyber operations, pressure by migration and even instrumentalising organised crime. The use of economic warfare and negative influence has grown and is very likely to increase further.<sup>5</sup> Hybrid actors attempt to influence events and developments in other countries with a mixture of non-military and military means and methods. Their execution mostly lies within the purview of national intelligence services – although non-state actors engage in hybrid activities as well.<sup>6</sup>

The execution of such operations happens on multiple levels within the target state and is usually comprised of a variety of interwoven measures, a combination of statecraft tactics with non-typical means such as criminality, which – independently and on the surface – appear to be harmless. But taken together they conspire to achieve nefarious ends. These ends are usually the political or societal disruption of the target and the subversion of political processes and policy

making to the advantage of the perpetrator. Among the better known examples of such a strategy are the many disinformation campaigns that target audiences worldwide, mainly through social media, to sow internal dissent and achieve distorted political outcomes. Currently, the consumption of Russian disinformation and fake news, for instance, has been at a higher rate than before the war against Ukraine.<sup>7</sup> Another common hybrid threat has been the use of cyberattacks to put financial pressure on target nations by disrupting data flows and communications.

More elaborate hybrid threats consist of long-term influence operations. The Indian government, for instance, set up a campaign over more than 15 years through an extensive network of think tanks, cultural institutions, opinion makers, and various media channels to promote a positive image with the United Nations and the EU to influence decision-making in India’s favour.<sup>8</sup> The European Parliament recently published a report detailing the various ways in which foreign actors, such as strategic opponents of Europe like Russia and China, interfere with political processes in the member states and within the institutions of the EU by instrumentalising politicians and influential people.<sup>9</sup> Adversaries endanger strategic autonomy by acquiring significant parts of vital economic assets, such as ports, cutting-edge technology and critical infrastructure or natural resources – which then serve as means of coercion. Hybrid actors combine these tactics in

---

4 Len Scott, ‘[Secret Intelligence, Covert Action and Clandestine Diplomacy](#)’, *Intelligence and National Security* Vol. 19(2), 2004, p. 322-341.

5 Mark Galeotti, *The Weaponisation of Everything. A Field Guide to the New Way of War*, New Haven: Yale University Press, 2021, p. 97.

6 For an overview of intelligence services being the linchpin of covert action see for instance Michael Warner, *The Rise and Fall of Intelligence. An International Security History*, Washington D.C.: Georgetown University Press, 2014; Thomas Rid, *Active Measures. The Secret History of Disinformation and Political Warfare*, New York: Farrar, Straus and Giroux, 2020.

7 Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*, 22 June 2022, p. 15-22.

8 Gary Machado, Alexandre Alaphilippe, Roman Adamczyk and Antoine Grégoire, *Indian Chronicles: deep dive into a 15-year operation targeting the EU and UN to serve Indian interests*, EU DisinfoLab, 2020. For the Russian activities in this regard, see Vladislava Vojtíšková, Vit Novotný, Hubertus Schmid-Schmidfelden and Kristina Potapova, *The Bear in Sheep’s Clothing. Russia’s Government-funded Organisations in the EU*, Wilfried Martens Centre for European Studies, July 2016.

9 European Parliament, *Foreign interference in all democratic processes in the European Union*, 9 March 2020.

a deliberate strategy to produce effects in one domain by manoeuvring in other domains.<sup>10</sup> They obfuscate their activities by denial and deception. Denial is meant to hide information from the target to allow the operation to continue unhindered and to impair policy decision-making. Deception intends to mislead the public and policymakers towards choosing policy outcomes that are not in their best interests.

Foreign malign influence poses a danger to the strategic autonomy and position of the EU on the international stage by undermining and eroding the institution and individual member states, democracy and the rule of law in general, and the functioning of a multilateral world order. Because of the subtlety and the divergence of the means employed, these operations are complex and difficult to detect. Hence, an effective response to these threats is also difficult to achieve, because they exploit the differences between the public and private sectors, and the internal compartmentalisation within companies and government administrations. The challenges for the latter are to achieve coordination and synchronisation to be able to react comprehensively to negate and build up resilience against the negative effects of hybrid campaigns. That requires a coordinating structure, plus a doctrine on how one can retaliate against what.

The EU's strategic response to the full range of these threats is to design a Hybrid Toolbox which indexes all available countermeasures and facilitates the development of new ones, in order to surpass the different levels and departments across which these measures are sourced, in an integrated and coordinated framework. When a member state is the victim of a hybrid attack that constitutes an internationally wrongful act, it may legally resort to proportionate countermeasures. The EU seeks to support and complement member states with their response, if they so desire, through the EUHT. The European External Action

Service supports the European Council, where the Working Party on Enhancing Resilience and Countering Hybrid Threats is charged with implementing this framework. It can be used where member states find themselves in difficulties when trying to deal with a hybrid campaign by themselves, and would reinforce their efforts with the combined capabilities and expertise across the EU. The main added value of the EUHT is perhaps less in assisting individual member states with their national response, than in responding in the spirit of 'a hybrid attack against one is a hybrid attack against all'. One of the objectives of the Toolbox is to make the EU and its members more resilient, in order to strengthen deterrence by making them less easy targets. The other is to provide a doctrine to actively respond to and push back hybrid threat actors. The toolbox and rapid response teams would also be available to non-EU countries. Operationalisation was intended by the end of 2022, although this ambitious deadline no longer looks feasible to be met. The implementation of the framework is in full swing, however.

## Where are we now?

Three months after the adoption of the Strategic Compass, the Council published its conclusions on the implementation of the EUHT. These outline the guiding principles of making it work and list existing tools and mechanisms that could already be part of the toolbox, what is currently in development that could be included – such as the embryonic Foreign Information Manipulation and Interference Toolbox (FIMI).<sup>11</sup> More than 200 tools and measures have so far been identified as suitable for countering hybrid threats. The Council conclusions follow earlier initiatives, such as the mapping of measures at the EU level that are relevant to counter hybrid threats (2020), the Inventory of EU crisis management capabilities (2019), and a review of the 2016 Playbook on

---

10 David Betz, 'The Idea of Hybridity', in: [Hybrid Conflicts and Information Warfare](#), Ofer Fridman, Vitaly Kabernik & James Pearce (eds.), Boulder: Lynne Rienner Publishers, 2019, p. 10.

---

11 Council of the European Union, '[Council Conclusions on a Framework for a coordinated EU response to hybrid campaigns](#)', 2 June 2022.

countering hybrid threats. There is also the Hybrid Risk Survey which points out common risks, vulnerabilities, and capability gaps among the member states. Furthermore, there are already countermeasures in place, such as the Cyber Diplomacy Toolbox, which was adopted in 2017 to counter cyberattacks and cyber criminality. There is also a role envisioned for the Integrated Political Crisis Response (IPCR) mechanism, that is meant to support rapid and coordinated decision-making at the EU political level for major and complex crises, including acts of terrorism. However, the Cyber Diplomacy Toolbox and ICPR are to remain autonomous and independent from the Hybrid Toolbox.

The question is how to coherently collect all these different tools and mechanisms, spread out over different institutions and levels, in a coordinated structure which can be activated at the request of a member state subject to a hybrid attack. To this end a distinction was made between two levels. The *Framework for a coordinated EU response to hybrid campaigns* will consist of a set of procedures for decision-making that can be activated in the event of a hybrid campaign taking place. This framework sets up the *Hybrid Toolbox* which is a catalogue of measures to mitigate and terminate the impact of a hybrid campaign at its earliest possible stage.

However, at the level of the EU institutions themselves, the development of the hybrid as well as the FIMI toolboxes is creating some anxiety. Many of the instruments that have been listed as desirable for the hybrid toolbox are established tools and mechanisms that currently fall under the European Commission Directorates responsible for their respective areas. These departments are not enthusiastic about what they perceive as potentially losing control over their instruments to the EEAS or Council bodies, although the intent is not control but coherence and coordination.<sup>12</sup> There are also legal difficulties, as many available tools are comprised of EU directives which fall squarely under the competence of the Commission. The latter is therefore in favour

of comprehensively cataloguing all available means to counter hybrid campaigns, as long as control over their use remains with the institution where those means originated and are regulated. On the other hand, that poses problems for the effective use of those means.

The EUHT is to be complemented by Hybrid Rapid Response Teams to enable a rapid deployment of relevant expertise adaptable to the threat. The teams are envisioned to be a combination of relevant sectoral national and EU expertise to deal with the situation on a case-by-case basis, thereby assisting national authorities. Their implementation is a matter concerning the mandate, spectrum, composition and scope of such teams, as well as their deployment. Again, the Cyber Diplomacy Toolbox serves as good practice upon which these hybrid response teams can be based. It provides for emergency response teams which are on permanent standby and can assist member states as soon as an agreement on such assistance is reached. Also serving as a model are the NATO Counter Hybrid Support Teams which were deployed in Lithuania in 2021 and Montenegro in 2019.<sup>13</sup> Because the assistance that was needed in those two countries mainly involved non-military capabilities, the added value of the EU teams would be that they fill in the gaps that NATO response teams have. In short, the EU would complement rather than duplicate NATO expertise. Also, as NATO teams can only be deployed within the territory of members of the Alliance, the EU rapid response teams could, as CSDP missions, support third countries needing counter-hybrid assistance.

Tabletop exercises and scenario-based policy discussions are ongoing to enhance a common understanding and to identify lessons, focusing on practical modalities for further implementation. Many questions remain open that are not easy to answer, since they concern problems that stem from two main issues: the differences in vision between member states about the

---

12 Information based on interviews.

---

13 The Baltic Times, '[NATO Counter Hybrid Support Team arrives in Lithuania](#)', 7 September 2021.

framework, and the difficulties arising from putting its workings in practice. These will be considered below.

## Diverging views and ambitions

As noted in a working paper by the Hybrid Centre of Excellence, the Strategic Compass must be “politically digestible” and “realistically implementable”.<sup>14</sup> The implementation of the Hybrid Toolbox is a good example of how member states can diverge on policy which translates into different levels of ambition. The attitudes of the member states allow certain fault lines to be discerned which correspond to either their threat perception or their posture towards the EU. Whereas all member states recognise the need for and the utility of a concerted response to hybrid threats, not all are enthusiastic about the EU institutions reaching further within the sovereign competence of national security. Although the dividing lines are not that clear-cut.

A number of member states have taken the lead towards fulfilling the ambitions driving the development of the EUHT. Likely as a result of their proximity to the main aggressor (the Russian Federation), northern countries drive the process and want the EU to complement and fortify their capacities. The Netherlands, Finland and Denmark have shown themselves to be quite proactive, persuading other countries to jointly write working papers or co-signing them and further outlining their thoughts on how the full potential of the hybrid toolbox could be achieved. In the second half of 2022, the Czech Presidency stimulated the preparatory work and also the upcoming Swedish Presidency demonstrates a constructive attitude. Other countries, for reasons that are not always clear, have shown some reluctance in realising a properly working EUHT. Aside from Euroscepticism, certain member states have shown recalcitrance, such as Austria, France, Hungary, Italy,

Luxembourg, Malta and Croatia. Their reasons stem from a limited threat perception, a lack of personnel to meet the expectations in dealing with the problem, or economic reasons such as social media platforms fearing repercussions for their activities and pressuring their host nations to keep things amenable.<sup>15</sup> Others suspiciously guard national security as an exclusive sovereign competence not to be encroached upon by Brussels. In general, there is something of an east-west/north-south divide in terms of support for the EUHT, with the northern and western member states being proactive and the eastern and southern nations showing little engagement. It must also be noted, however, that certain nations, like Belgium, remain on the fence and are currently awaiting developments in order to take a position in the debate, so far only carefully signing on to positions by more active nations but otherwise pushing for more clarification of the issues at hand.

The relationship of the EUHT with existing capabilities within NATO is also a matter for discussion. The proactive nations believe in making the toolbox work to its full potential. They adhere to the closest possible cooperation with NATO in terms of finding synergies, leveraging complementarity, and avoiding duplications. However, political and philosophical differences might stand in the way of fulfilling the potential of a true joint EU/NATO response capability that is well adjusted to one another’s strengths and abilities. In the context of the Rapid Response Teams, for instance, NATO already has a developed capability upon which the EU teams are modelled, as mentioned above; opinions are therefore divided on whether the EU teams should have a different approach or aim towards maximum compatibility with NATO teams and expertise, some of which will likely overlap with whatever the EU develops. Ways have to be found to complement and reinforce each other’s capabilities, rather than compete or work in parallel ways. Again, the first step would be to hold exercises to expose the discrepancies.

---

14 Rasmus Hindrén, *Calibrating the Compass: Hybrid Threats and the EU’s Strategic Compass*, Hybrid Centre of Excellence Working Paper 12, October 2021, p. 16.

---

15 Information based on interviews.

Another important issue regarding efficient reaction revolves around sanctions. The Cyber Diplomacy Toolbox allows for not only imposing sanctions that are country-specific but can be applied to particular entities or natural persons as well (smart sanctions). The European Parliament has also advocated a cross-sectoral and asymmetric sanctions framework.<sup>16</sup> As argued by researchers evaluating the toolbox, “the personalised character better suits the present dynamics in the cyberspace in which states often rely on non-state actors – so-called proxies – to project their strategic interests.”<sup>17</sup> It would be beneficial to do the same with the EUHT and provide for targeted sanctions as the primary actor in hybrid campaigns is not necessarily the state but the regime running that state.<sup>18</sup> Again, flexibility is important for counter-hybrid sanctions to be smart and effective. But sanctions are a predominantly political problem, hence complicating their use as part of a counter-hybrid approach. Sanctions imply attribution, and attributing cyber or hybrid attacks is undoubtedly the most contentious issue in making the EUHT work. Attribution is two sides of the same coin: on the one side, there is attribution as a political tool (often referred to as a ‘joint/coordinated attribution’) and, on the other, attribution as a part of the decision-making process (technical attribution). The latter is based on intelligence assessment and is done for the sake of taking effective decisions. It should be one of the goals of the decision-making process to determine who is the actor behind the incidents in question, i.e. technical attribution. Coordinated public attribution should then be dealt with carefully and only after broad consideration, as a political decision which should not delay the taking of immediate countermeasures. Attribution therefore should be seen as being separate

from triggering the EUHT and subsequent action, which is the next subject.

## How to decide on using the toolbox?

The Council conclusions stipulated guiding principles but not when and how the EUHT is to be activated. Any agreement on the main characteristics of the provisions for invoking the EUHT should consider the existing legal basis, the institutional framework and the need to provide quick and efficient decisions. To advance the preparatory work, the Czech Presidency circulated a set of questions concerning these issues. The replies pointed out similarities in member states’ thinking on a number of topics, while indicating certain discrepancies.

First, there is the matter of the legal basis for the EU to act in this field, most of which remains squarely in the sovereign domain of the member states. The treaties regulating the Union do not provide the concrete legal bases to adopt measures to counter cyber or hybrid threats, but two articles come to mind. The mutual assistance clause (Treaty of the European Union (TEU), Article 42.7) and the solidarity clause (Treaty on the Functioning of the European Union (TFEU), Article 222) are options to be considered, provided that the conditions for their application are met. A member state may choose to invoke Article 42.7 to call on the EU to provide aid and assistance. The text of Article 42.7 specifically points to (other) member states to provide aid and assistance. The EU institutions could, if so requested, coordinate and facilitate activities, but the leading role clearly lies with the member states.<sup>19</sup> The solidarity clause is a special provision obliging member states to assist each other in the event of man-made or natural disasters when responding to them exceeds national capabilities. Migration, border

---

16 European Parliament, *Foreign interference in all democratic processes*, 2020, p. 137.

17 Yuliya Miadzvetskaya and Ramses Wessel, ‘[The Externalisation of the EU’s Cybersecurity Regime: the Cyber Diplomacy Toolbox](#)’, *European Papers* Vol.7(1), 2022, p. 431.

18 Michael Warner, ‘[A Matter of Trust: Cover Action Reconsidered](#)’, *Studies in Intelligence* Vol.63(4), 2019, p. 34.

---

19 For a further explanation of Article 42.7, see: Bob Deen, Dick Zandee, Adája Stoetman, [Uncharted and uncomfortable in European defence – The EU’s mutual assistance clause of Article 42\(7\)](#), Clingendael Report, January 2022.

protection (Articles 67.2 and 80 TFEU), and financial assistance after natural disasters or in exceptional circumstances (Art. 122 TFEU) also refer to solidarity. Another option would be Article 329.2 of the TFEU that provides for the possibility to cooperate more closely within the Common Foreign and Security Policy (CSDP), if authorised by the Council.<sup>20</sup> The practical problem with these provisions is that, aside from arguably the solidarity clause, their actual application remains vague. Without a concrete implementing framework, it is not clear, however, how these treaty provisions can be used on their own to address the events for which they are intended. So, this should be clarified.

Member states have stressed that the added value of the EUHT would be to provide an ‘umbrella’ framework, facilitating the coherent application of relevant internal and external tools to strategically respond to hybrid campaigns. In this view, the activation of the EUHT would in every case result in a tailored approach, going beyond merely responding to hybrid activities, but also mitigating latent activities by strengthening resilience. Its guiding principles should be subsidiarity, complementarity and proportionality, and its components can be grouped in the following five categories:

- 1) preventive measures (capacity building);
  - 2) cooperative measures (coordination with like-minded countries and coordination with NATO);
  - 3) stability measures (diplomacy, CSDP missions and operations, strategic communication);
  - 4) restrictive measures (attribution and sanctions);
  - 5) assistance and solidarity measures.
- With these categories the EUHT follows the example of the Cyber Diplomacy Toolbox.

With the framework in place, how can EU countermeasures be triggered? Naturally, countermeasures can only be activated provided that a hybrid attack is discovered. What thresholds will be determined to be sufficiently grave for a member state to

invoke the Framework’s procedures? Apart from clear-cut large-scale hybrid attacks such as the cyberattack on Estonia in 2007, hybrid campaigns are essentially denial and deception operations across complex domains in constant interaction with each other. They will only generate spurious signals which will be incremental and rarely tangible or sufficiently clear-cut to eliminate doubt about what they constitute. This underlines the importance of enhanced situational awareness, more about which below.

According to the implementing guidelines,<sup>21</sup> the activation process would go as follows:

- 1) When one or several incidents that could be part of a hybrid campaign have been detected or have been brought to the attention of member states by the Commission or the High Representative, a partner country or international organisation;
- 2) Member state(s) request that the Council (e.g. through the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats) discuss the issue. The Commission and the High Representative are invited to start preparing possible options;
- 3) The Hybrid Fusion Cell provides strategic foresight and comprehensive situational awareness, notably to assess the origin and features of the hybrid threats and campaigns. Other relevant EU institutions, bodies and agencies as well as CSDP missions and operations and international partners, and security services could complement where appropriate, including through open source information;
- 4) The Commission and the EEAS as well as member states can also be invited to contribute to the situational overview with updates on their ongoing activities;
- 5) The Commission and the EEAS issue proposals and recommendations in an options paper, and also provide timely information about measures taken within their scope of competence;

---

20 Miadzvetskaya and Wessel, *The Externalisation of the EU’s Cybersecurity*, 2022, p. 437.

---

21 Implementing Guidelines for the Framework for a Coordinated EU Response to Hybrid Campaigns.

- 6) The Council receives and discusses these proposals;
- 7) The Hybrid Working Party prepares recommendations and proposals for the Committee of the Permanent Representatives of the Governments of the Member States to the European Union (Coreper), the Council's main preparatory body. If needed, the Council's Political and Security Committee (PSC) may deliberate on the measures decided on that fall within its mandate;
- 8) The Council takes a decision on implementing a measure. On a case-by-case basis, the PSC may be involved;
- 9) Member states and EU bodies implement decisions;
- 10) The Council follows up on the implementation and relevant lessons learned;
- 11) Member states may request to revisit the relevant steps of the process should additional measures be required.

This step-by-step approach raises a number of bureaucratic issues. Not all measures under this Framework require a separate decision by the Council, as they may be autonomous depending on their legal basis and the decision-making mechanisms. For measures not requiring a Council decision, information will be given by the Commission and the High Representative on the tools and measures that are already in use or that may be employed. Based on the scope and nature of the hybrid threat and the external actors in question, the Political and Security Committee (PSC) may also deliberate on the case. Relevant regional and thematic Council working groups can be involved as well.

Despite the purpose of the Framework to provide coordination with consistency and coherence, there are still different procedures being applied. If the hybrid campaign is part of a crisis for which the integrated political crisis response (IPCR) arrangements have been activated, the independent IPCR procedures will apply. That also goes for the Cyber Diplomacy Toolbox which operates autonomously, in line with its own rules and procedures, and also has a separate Cyber Working Party. That begs the question: what should the decision-making process look like when

a cyber incident is part of a hybrid or FIMI campaign? Most hybrid campaigns would have at least some cyber components, so the relationship between the two toolboxes is very important from a practical perspective. Member states would need the flexibility to decide which toolbox to use. In cases where a cyber incident is identified and only later is it discovered to potentially be a part of a broader hybrid campaign, there would follow a bureaucratic series of discussions between both working parties to examine whether the connection of the cyber tools is relevant. When they agree that this is the case, further examination in both working groups should be done in close coordination. A similar approach should be applied in cases when a cyber incident is identified only later as part of a wider hybrid campaign. The Hybrid Working Party should then consider, perhaps jointly with the Cyber Working Party, the relevance of such an incident for the wider campaign. Member states can decide which toolbox they prefer to apply, while they can also be used simultaneously.

This all sounds rather complicated and seems to involve a lot of deliberation and to and fro. The question is how time-consuming this will be and whether this complexity will not defeat the goal of consistent and coherent coordination. On balance, this process runs a great risk of quickly being mired in bureaucratic processes and arguments, which would reduce the effectiveness of decision-making, in particular rapid decision-making, which is essential in responding to hybrid campaigns. For the sake of efficiency, some of the steps above might be merged and emergency cases will require speediness and less or faster deliberation. Joint sessions are key to dealing with this issue, while cooperation and coordination should be exercised regularly.

## Suggestions for increasing effectiveness

Aside from the necessity of having optimal internal procedures for the EUHT to be effective, there are several other suggestions which should be taken into account when



planning the implementation of the EU's counter-hybrid framework.

Crucial to this undertaking is achieving a shared situational awareness to the highest degree possible. To this end the Strategic Compass underlines the importance of the optimal functioning of the EU's civilian intelligence organism, called the Single Integrated Analysis Capacity (SIAC). Of particular importance is its Hybrid Fusion Cell which combines civil and military elements to detect and assess threats and their sources.<sup>22</sup> However, in order for this to work properly, the intelligence arrangements within the EU have to be drastically improved.

As with earlier initiatives, information sharing remains problematic. The evaluation of the Cyber Diplomacy Toolbox, for instance, noted a number of issues in this regard. Pursuant to the treaties, member states have no obligation to share if they deem it contrary to their national security to do so. The EU's information position thus remains for the most part dependent on the goodwill of member states intelligence services. There is the problem of trust among the intelligence services feeding information into the SIAC. Furthermore, the need to justify action puts a disproportionate emphasis on the prerequisite of open source information so that member states would have no reluctance when it comes to sharing.<sup>23</sup> This creates another problem. As hybrid campaigns are riddled with ambiguous and intangible intelligence data, analysis is barely possible without classified information of a highly sensitive nature that would be difficult to share and validate.<sup>24</sup> The information-sharing problems fundamentally challenge the principle that

there is common agreement on threats and threat actors in order to take action, as outlined in the Council conclusions. Enhancing situational awareness and improving detection capabilities also imply that the EU's intelligence bodies have to invest in a broader geographic coverage and strive towards the most intensive cooperation with NATO, which suffers from the same pathologies regarding intelligence arrangements. Additionally, the problem of exchanging classified information between NATO and the EU remains unsolved.

As mentioned above, thresholds will be needed to invoke the help of the EUHT upon the detection of a hybrid campaign. In addition to situational awareness, a common understanding and the availability of a taxonomy of indicators are required. The European Centre of Excellence for Countering Hybrid Threats offers 13 domains across which hybrid threats can materialise (see figure 1). These domains as well as the actions and tactics that can be taken within them can be visualised in the order of their degree of intervention, intrusiveness and seriousness, which could serve as a ladder of escalation (see appendix),<sup>25</sup> and provide member states with the means to assess when an attack is serious enough to request the activation of the EU framework.

Currently, the relevant policy documents make little mention of the ability to anticipate hybrid threats. Preventing them places the burden on strengthening deterrence – immediately squaring the circle even by making resilience the main deterrent dissuading an adversary from initiating a hybrid campaign – rather than becoming proactive. Hence, it would seem that the focus lies on a reactive approach. In other words, a hybrid threat has to be already ongoing and subsequently detected for a member state to invoke assistance at the EU level. However, from a counterintelligence standpoint, there is something to be said for making it possible to activate the EUHT on

---

22 Council of the European Union, *A Strategic Compass for Security and Defence*, March 2022, p. 22.

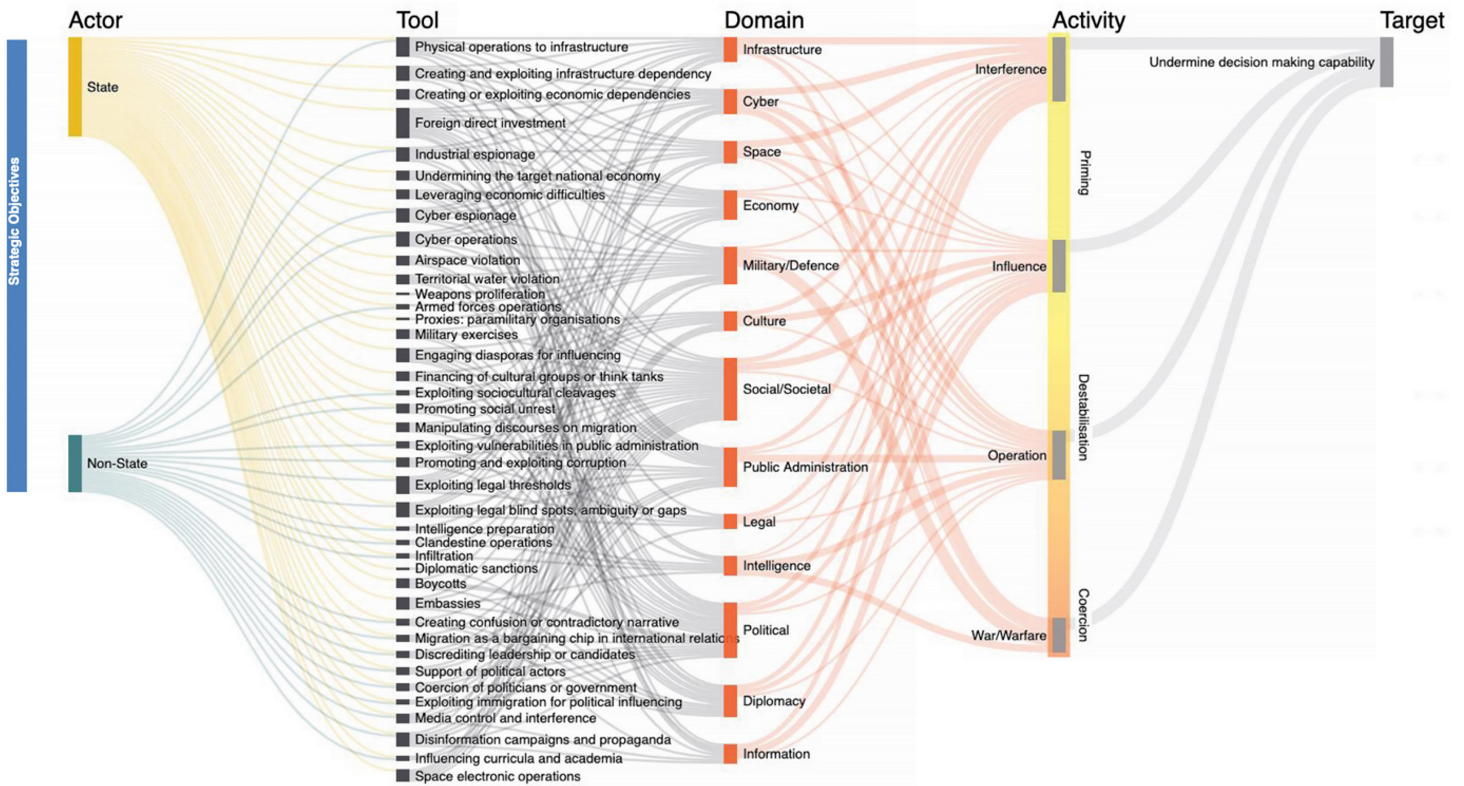
23 Miadzvetskaya and Wessel, *The Externalisation of the EU's Cybersecurity*, 2022, p. 436.

24 James Bruce and Michael Bennett, 'Foreign Denial and Deception: Analytical Imperatives', in: *Analyzing intelligence. Origins, Obstacles, and Innovations*, Roger George & James Bruce (eds.), Washington D.C.: Georgetown University Press, 2008, p. 125.

---

25 See Loch K. Johnson, 'On Drawing a Bright Line for Covert Operations', *The American Journal of International Law* Vol.86(2), April 1992, p. 286.

**Figure 1** Taken from Giannopoulos, Smith & Theodoridou, *The Landscape of Hybrid Threats*, 2021, p. 13.



an *ex ante* basis, that is, as soon as there are credible indications that a hybrid campaign is about to be unleashed or in its early stages of deployment. The most efficient way to counter hybrid operations is by nipping them in the bud or turning them against the aggressor in pure counterintelligence fashion. To achieve this goal the situational awareness will have to focus more strategically on the motives and objectives of adversaries and their intentions, as well as the vulnerabilities at EU and national levels which they would seek to exploit.<sup>26</sup> With the proper sensors and analysis capabilities, there are better assessment possibilities to determine what threats are being shaped against individual member states or the EU itself, and to devise the right integrated response.

26 Robert Clark and William Mitchell, *Deception. Counterdeception and Counterintelligence*, Washington D.C.: CQ Press, January 20118, p. 34-38.

## Conclusions and recommendations

In parallel with the complexity of dealing with hybrid campaigns, implementing the EU Hybrid Toolbox is not an easy matter. Many options are already available in the EU – such as the Cyber Diplomacy Toolbox – but the main challenge will be to enable a fast and coherent response. The implementation will be a real test of the EU’s ability to act across the divisions between internal and external security sectors as well as across different policy areas.<sup>27</sup> If done in the right way, it would establish the EU as a comprehensive and powerful actor to deal with those complex crises which are beyond the capabilities of individual states, and improve the chances of countering the hybrid attempts undermining international order.

27 Hindrén, *Calibrating the Compass*, 2021, p. 17.

## Opportunities

- The EU Hybrid Toolbox would allow hybrid threats to be dealt with in a coordinated fashion with the full force of the EU's power as soon as possible rather than when they have turned into a fully-fledged crisis. This would also position the EU more strongly as a global partner for countering attacks on the international order. There is an opportunity here to endow the relevant treaty articles with a clearer mandate and concrete operationalisation to make it possible for the EU to act.
- There is a great potential to enhance situational awareness. The EUHT would provide the resources and capabilities ensuring the ability to detect hybrid threats in order to inform the decision-making process.
- The information position needed for the EUHT to be effective is certainly an opportunity to leverage individual member states' capabilities with a performative EU intelligence capability, which would be a critical advantage. This requires more robust sharing arrangements that increase the level of trust between the contributing partners.
- A common understanding and the availability of a taxonomy of indicators are required. It is incumbent upon the Hybrid Working Party to clearly delineate the thresholds to determine when a hybrid attack or campaign is ongoing, while at the same time allowing for flexibility that reflects the dynamics of hybrid warfare and the adaptability of aggressors.
- Strategically, the EU's counter-hybrid response should strive towards maximum cooperation and compatibility with NATO capabilities. Regular exercises, including joint exercises with NATO, can streamline the close cooperation in order to complement and mutually enforce the capabilities of both organisations.
- The question remains open which entity is to have this coordinating role without infringing on existing competences and administrative sensitivities. To solve this issue, an executive-level position might be called for which can coordinate all sectors involved and be responsible for the viability of the EUHT.
- The differences in opinion among member states underline the importance of having a tailored approach which is also adjusted to the specific regional characteristics, as hybrid campaigns will have different aspects according to their geographical direction. Making the EUHT as adaptable as possible will ensure its continued relevance and effectiveness. It will be important to maintain the dynamic aspect of the EUHT and FIMI toolboxes, i.e., being very flexible and continuously updated.
- That the concept of the EUHT contributes mainly to enhancing resilience is most valuable. But it would be an even more effective instrument if it also enabled anticipation through an *ex ante* approach.
- The mechanisms in the framework can also be valuable for facilitating collective attribution. Every member state should maintain its own methods and procedures for attribution, which is a political, sovereign decision and should be separate from activating the EUHT.
- If the proactive member states, and others continue to stimulate cooperation among themselves, they prove the increased effectiveness and added value of a joint effort in countering hybrid campaigns.
- The existing coalitions of member states – such as Denmark, Finland, Sweden and The Netherlands – must act together to convince the sceptical nations of the benefit of jointly having an efficient counter-hybrid framework. The willing could then continue to raise awareness and stimulate political will. The challenges need to be discussed, analysed, game planned and exercised. Especially, lessons learned from exercises can help to demonstrate the need and relevance of this initiative. Also, the instances when rapid response teams and EU expertise have already been deployed, such as in Montenegro and Lithuania, can be studied for points of improvement and good practices.
- Strategic communication with clear, strong, proactive and consistent messaging accompanying EU responses to hybrid threats, reinforce their impact and shape the perception of the EU's intent.

- Finally, the implementing guidelines must be reviewed regularly to evaluate if they provide the correct mechanisms for utilising the toolbox in a manner that reflects and mitigates the concerns of member states about EU powers, in order to get as many member states as possible on board.

### Pitfalls

- The EU Hybrid Toolbox has a high level of ambition that does not necessarily correspond with what the EU is functionally and operationally able to achieve as the record of its security and defence agenda shows. The geopolitical sensitivity is high and, logically, it will be very difficult to align the member states and even the institutions within the EU.
- The toolbox seems to focus on a reactive approach, whereas it should also be proactive to achieve maximum preventive and deterrent effect.
- Situational awareness and intelligence arrangements have to be the primary concern, but there are various obstacles, such as the vagaries of intelligence analysis and its difficulties of interpretation. Another problem is the principle of aiming for full agreement on the intelligence before it can be acted upon, which invites classical intelligence failure pathologies, such as groupthink and consensus mania, guaranteeing flawed analysis and response. Issues of trust and the exchange of classified information will also remain difficult to overcome.
- There is potential but at the same time much difficulty regarding decision-making. It will be crucial for the effectiveness of the hybrid toolbox that procedures are clear and unequivocal, while at the same time their flexibility must also be guaranteed, emulating the adapting capabilities of a learning opponent. Without the necessary pressure from within the Council it will be problematic to align the different stakeholders in a structure that guarantees coherence and coordination. For this a clear mandate will have to be put forward.
- The division between independent arrangements, all of which nonetheless serve to deal with the same security challenge, remains arduous. How credible will the EU be in having three autonomous sets of procedures in such a case: the Cyber Diplomacy Toolbox, the Hybrid Toolbox, and the Integrated Political Crisis Response mechanism? Questions regarding their relationship and their governance endanger the operationalization of the EUHT by making their activation complicated and time-consuming.
- The different national positions towards the development of the EUHT risk rendering the toolbox a rhetorical concept with limited or no practical use. The recalcitrance of sceptical member states might result in a dilution of not only the tools that comprise the EUHT but also of the decision-making process. Bureaucratic impediments and terminology disputes may render the toolbox ineffective. The resulting countermeasures could be too vague and therefore not useful in the event of an actual hybrid campaign that requires mitigation at the EU level. As such, they risk being superseded by existing crisis response mechanisms. Such an outcome would be contrary to the purpose of the EUHT.

Many efforts have to be made in order to enable effective EU responses to hybrid campaigns. Success in the implementation of the EU Hybrid Toolbox will contribute to strengthening Europe's capacity to better defend against and deter attempts to undermine its international position and politico-economic clout, and strengthen international norms and values. It will benefit all those working together to blunt the forces of global disorder.

## APPENDIX: escalation ladder






Taken from Loch K. Johnson, 'On Drawing a Bright Line for Covert Operations', *The American Journal of International Law* Vol. 86(2), 1992, p. 286.

A PARTIAL ESCALATION LADDER OF STRATEGIC INTELLIGENCE OPTIONS	
EXTREME OPTIONS	<p>THRESHOLD FOUR</p> <p>38. Use of chemical-biological, other deadly agents (PM)            37. Major secret wars (PM)            36. Assassination plots (PM)            35. Small-scale coups d'état (PM)            34. Major economic dislocations; crop destruction (E)            33. Environmental alterations (PM/E)            32. Pinpointed relation against noncombatants (PM)            31. Torture (POL/C)            30. Hostage taking (POL/C)            29. Major hostage-rescue attempts (PM)            28. Theft of sophisticated weapons or materiel (PM)            27. Sophisticated arms supplies (PM)</p>
HIGH-RISK OPTIONS	<p>THRESHOLD THREE</p> <p>26. Massive increases of funding in democracies (POL)            25. Disinformation against democratic regimes (P)            24. Disinformation against autocratic regimes (P)            23. Small-scale hostage-rescue attempts (PM)            22. Training of foreign military forces for war (PM)            21. Limited arms supplies for offensive purposes (PM)            20. Limited arms supplies for balancing purposes (PM)            19. Economic disruption without loss of life (PM)            18. Large increases of funding in democracies (POL)            17. Massive increases of funding in autocracies (POL)            16. Large increase of funding in autocracies (POL)            15. Sharing of sensitive intelligence (C)            14. Embassy break-ins (C/CE)            13. Truthful, contentious information in democracies (P)            12. Truthful, contentious information in autocracies (P)            11. High-level, intrusive political surveillance (C)            10. High-level recruitment and penetrations (C/CE)</p>
MODEST INTRUSIONS	<p>THRESHOLD TWO</p> <p>9. Low-level funding of friendly groups (POL)            8. Truthful, benign information in democracies (P)            7. Truthful, benign information in autocracies (P)            6. Stand-off TECHINT against target nation (C)            5. "Away" targeting of intelligence officer (C/CE)            4. "Away" targeting for intelligence gathering (C)</p>
ROUTINE OPERATIONS	<p>THRESHOLD ONE</p> <p>3. Sharing of low-level intelligence (C)            2. Ordinary embassy-based observing and conversing (C)            1. Passive security measures; protection of leaders (S)</p>
Key:	<p>C = collection of intelligence            S = security (a passive form of counterintelligence)            CE = counterespionage (an active form of counterintelligence)            P = covert propaganda (a form of covert action)            POL = political covert action            E = economic covert action            PM = paramilitary covert action</p>

### About the Clingendael Institute

Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.

[www.clingendael.org](http://www.clingendael.org)  
[info@clingendael.org](mailto:info@clingendael.org)  
+31 70 324 53 84

 @clingendaelorg  
 The Clingendael Institute  
 The Clingendael Institute  
 clingendael\_institute  
 Clingendael Institute  
 Newsletter

### About the author

**Kenneth Lasoen** is Research Fellow at the Security Unit of the Clingendael Institute and lectures Intelligence and Security at the University of Antwerp. He specialises in national security and intelligence, counterintelligence and counterterrorism.

**Disclaimer:** The research for and production of this policy brief have been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defense.