



Council of the  
European Union

124837/EU XXVII. GP  
Eingelangt am 14/12/22

Brussels, 14 December 2022  
(OR. en)

15880/22

HYBRID 117	JAIEX 105
DISINFO 104	AUDIO 134
INST 453	DIGIT 235
AG 157	INF 213
PE 149	COSI 322
DATAPROTECT 357	CSDP/PSDC 881
JAI 1658	COPS 601
CYBER 401	POLMIL 306
FREMP 262	PROCIV 153
RELEX 1708	IPCR 118

#### OUTCOME OF PROCEEDINGS

---

From:	General Secretariat of the Council
To:	Delegations
Subject:	Implementing guidelines for the Framework for a coordinated EU response to hybrid campaigns

---

Delegations will find in the Annex the above-mentioned Council conclusions approved by the Council on 13 December 2022.

## IMPLEMENTING GUIDELINES FOR THE FRAMEWORK FOR A COORDINATED EU RESPONSE TO HYBRID CAMPAIGNS

### I. Introduction

The Strategic Compass, approved by the Council on 21 March 2022 and endorsed by the European Council on 24 and 25 March 2022, underlines the need to develop in 2022 an *EU Hybrid Toolbox* ('EUHT') in the course of 2022. The EUHT should bring together existing and potential new instruments and provide a framework for a coordinated response to hybrid campaigns affecting the EU and its Member States and partners; it should also include preventive, cooperative, stability, restrictive and recovery measures and strengthen solidarity and mutual assistance. In addition, the Strategic Compass emphasised the need to develop in 2022 the *Foreign Information Manipulation and Interference Toolbox* ('FIMI toolbox'), which will strengthen our ability to detect, analyse and respond to that threat, including by imposing costs on perpetrators.<sup>1</sup>

The *Framework for a coordinated EU response to hybrid campaigns* together with the implementing guidelines are the key components of the EU Hybrid Toolbox, which is an all-encompassing concept ensuring an integrated, strategic, operational and systematic approach to hybrid campaigns covering various domains.<sup>2</sup> As the first formal step in developing this initiative the Council conclusions on a Framework for a coordinated EU response to hybrid campaigns of 21 June 2022 introduced a framework for a coordinated response to hybrid threats and campaigns affecting the EU, Member States and partners.<sup>3</sup> The Framework should also be used to address foreign information manipulation and interference (FIMI). The Council called on the Member States, the Commission and the High Representative to give full effect to the development of the Framework, putting in place implementing guidelines as the second step. These implementing guidelines are intended to address the tasks identified above.

<sup>1</sup> Council conclusions on a Framework for a coordinated EU response to hybrid campaigns (ST 10016/22).

<sup>2</sup> As specified in Giannopoulos, G., Smith, H., Theocharidou, M., *The Landscape of Hybrid Threats: A conceptual model*, European Commission, Ispra, 2020, PUBSY No. 117280.

<sup>3</sup> In line with the Partner chapter of the Strategic Compass.

The main aim of the implementing guidelines is to give full effect to the *Framework for a coordinated EU response to hybrid campaigns*, in particular when considering and preparing comprehensive and coordinated EU responses to such hybrid campaigns, using existing and potential new tools.

The implementing guidelines: (a) should contribute to a faster and better decision-making process, taking into account the rapidly evolving threat landscape and involving all relevant decision-makers; (b) should enable a comprehensive cross-sectoral assessment of challenges and response options on the menu; (c) should facilitate coordination and coherence in the implementation of tools and measures; (d) should include a follow-up process to assess the effectiveness of the implementing guidelines themselves and discuss next steps on the basis of expertise developed in the relevant Council preparatory bodies.

Decisions on a coordinated EU response to hybrid campaigns will be guided by the principles already agreed by the Council in its conclusions on the Framework. The main principles stipulate that the decisions should:

- serve to protect democratic values, processes and institutions, as well as the integrity and security of the EU, its Member States and their citizens, and its strategic interests, including the security of partners in our neighbourhood and beyond;
- respect international law and protect fundamental rights and freedoms, and support international peace and security;
- provide for the attainment of the objectives of the Union, in particular the Common Foreign and Security Policy (CFSP) objectives, as set out in the Treaty on European Union (TEU), and the objectives set out in the Treaty on the Functioning of the European Union (TFEU), as well as the procedures required for their attainment;
- be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of each particular hybrid campaign;

- be based on a shared situational awareness among the Member States and correspond to the needs of the specific situation at hand;
- take into account the broader context of the EU's external relations with the state concerned by the response.<sup>4</sup>

### **Interaction of sectorial sets of measures and tools**

Given their multidimensional nature, hybrid campaigns can affect a broad range of domains. Consequently, close interaction and consistency needs to be ensured between existing and potentially new sets of measures as well as those currently being developed. This requires cooperation and coordination between and within relevant constituencies and preparatory bodies within the Council through appropriate mechanisms based on existing procedures and established practices. The EEAS and the Commission services should continue to keep the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats ('HWP ERC-HT') informed about their new sectoral or geographical initiatives seeking to address hybrid threats or campaigns.

### ***Cyber Diplomacy Toolbox***

**The Cyber Diplomacy Toolbox (CDT)** counters cyber security threats and could contribute to the EU's response to a hybrid campaign, in line with its own rules and procedures. Complementarity between the CDT and the EU Hybrid Toolbox should be ensured.

Member States should decide whether they prefer to activate the CDT and/or the EU Hybrid Toolbox when both cyber as well as hybrid elements are present in a hostile campaign against the EU, its Member States or, if agreed, partners. Both toolboxes can be used simultaneously given the specific range of tools they encompass.

---

<sup>4</sup> Council conclusions on a Framework for a coordinated EU response to hybrid campaigns (ST 10016/22).

The relevant preparatory bodies of the Council should consult each other on a coordinated EU response when seeking to address a hybrid campaign with cyber elements or a cyber attack that is part of a broader hybrid campaign. Intra-institutional coordination as well as joint meetings of relevant preparatory bodies of the Council should be organised in such cases. The procedures set out in the EU Treaties as well as in the implementing guidelines of both of the aforementioned toolboxes should be applied.<sup>5</sup>

### ***FIMI Toolbox***

As specified in the aforementioned conclusions<sup>6</sup>, the Framework should also be used to address foreign information manipulation and interference (FIMI). However, FIMI does not always need to appear as part of a hybrid campaign and can be present and addressed in itself.

The FIMI Toolbox should cover four dimensions: (1) situational awareness, (2) resilience building, (3) disruption/preparation and implementation of regulation and (4) CFSP measures. To enable use of the instruments under the first three categories, the Council should be kept informed on a regular and timely basis. Decision-making processes for the fourth category (CFSP measures) are governed by the Treaties; these measures are accordingly implemented through the Framework. All of these measures need to be brought together in a coherent manner, respecting the processes under existing mechanisms and instruments, and to inform and support the coordinated response of the European Union to such activity.

Following a briefing by the EEAS and/or the Commission services of actions taken under the first three dimensions of the FIMI Toolbox, any Member State, the High Representatives or the Commission may submit an initiative or proposal to the Council concerning actions to take. Any Member State is free to request or launch an initiative or to make a proposal at any time. On the basis of this initiative or proposal, Member States, the EEAS and the Commission services should continue exchanging relevant information enhancing situational awareness and discuss whether any action should be taken. For the measures that require a Council decision, the decision-making procedure to invoke the measures described below will be applied.

---

<sup>5</sup> Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities (ST 13007/17).

<sup>6</sup> Council conclusions on a Framework for a coordinated EU response to hybrid campaigns (ST 10016/22).

Many of the instruments to counter FIMI have been in existence and use for a long time, such as the EU's Rapid Alert System, the Code of Practice on Disinformation and the European Cooperation Network on Elections. Some of these instruments are related initiatives like the Digital Services Act and the Election Resilience Mechanism. International cooperation with key partners on foreign information manipulation and interference and disinformation will remain, under the FIMI Toolbox, an integral part of the EU's response across all four dimensions. Moreover, the FIMI Toolbox could provide support to partners across the globe to build capacity and capability for countering FIMI.

## **II. Situational awareness**

Awareness of hostile activity entails different interlinked phases of collection, analysis and distribution and includes the processes of monitoring, detection, threat assessment and ensuring shared situational awareness. The EU INTCEN Hybrid Fusion Cell with the support of EUMS Intelligence Directorate under the SIAC framework is the central entity providing situational awareness and plays the central role in analysing all-source information and providing intelligence assessments on hybrid threats. Previous assessments prepared by the EU INTCEN Hybrid Fusion Cell, such as the Hybrid Trend Analysis as well as long term trends and previous adversarial activities that have been attributed a high level of certainty, should be taken into account in the context of these processes.

Measures taken under the EU Hybrid Toolbox should be used in a coherent and consistent manner: this requires *inter alia* a comprehensive situational awareness of hybrid activities in different domains as early as possible and with the aim to mitigate and counter hybrid threats and campaigns once early signals thereof are detected. Maintaining up-to-date and continuous situational awareness is key in order to act swiftly and effectively when there is a need to activate the EU Hybrid Toolbox. Information flow therefore needs to be ensured, even when the EU Hybrid Toolbox is not activated. National security remains the sole responsibility of each Member State.

Ongoing exchange of information on hybrid threats and campaigns, with contribution appropriate EU institutions, bodies and agencies, CSDP missions and operations and, as and where appropriate, exchanges with international organisations, such as NATO, or international partners, such as the G7, will assist Member States with developing and maintaining a shared understanding about hybrid threats and campaigns and aid understanding of how these affect the EU, Member States and partners. Any Member State can provide additional information at any time. Updates on relevant activities of EU institutions are also important. This will contribute to the comprehensive situational awareness needed for decision-making on the measures under this Framework. Regular updates by the EU INTCEN Hybrid Fusion Cell should be envisaged so as to ensure that an early warning element and intelligence assessment is incorporated in the process.

Additional open source information analyses should also contribute to maintaining situational awareness on the hybrid threat landscape. The EEAS Rapid Alert System, as well as Member States sharing relevant situational updates and providing national assessments as part of awareness-raising activities within the relevant Council preparatory bodies, also have an important part to play in preparing decisions.

### **III. Process to activate the Framework and invoke measures**

The process starts when a Member State or the Commission services and/or the EEAS notify the Council of the need to discuss a hybrid threat or campaign which might lead to activation of the Framework by the Council. The initiative to start the process should trigger the immediate start of preparations for the discussion and the possible decision.

#### **Situational awareness as a part of the activation process**

Before any measure can be considered, timely and continuous sharing of information by all actors involved is an ongoing process and of key importance for the EU and its Member States.

Comprehensive situational awareness will enable the EU and Member States to take a collective decision on whether or not to use one or more measures from the EU Hybrid Toolbox, such as restrictive measures or any EU support for Member States' legal responses. Member States are not obliged, pursuant to the Treaties, to provide information or analysis when they consider it to be contrary to their national security interests.

The EU INTCEN Hybrid Fusion Cell will assume the leading role in aggregating all-source information, preparing an intelligence-based assessment and providing strategic foresight. This can be supplemented by other relevant EU institutions, bodies and agencies, CSDP missions and operations as well as partners, including the provision of open source information, where appropriate, while ensuring that all relevant information is also made available to the EU INTCEN Hybrid Fusion Cell.

The EEAS and the Commission services are invited to inform the Council about the tools and instruments that are already in use in relation to the case at hand and to provide timely follow-up reporting on their implementation and, where possible, information on the impact that actions taken are having/have had on the campaign.

### **Preparing a decision**

When one or multiple incidents that could be part of a hybrid campaign have been detected by Member States or have been brought to the attention of Member States and Presidency by the Commission or the High Representative, one or more Member States may request that the Council examine the issue. Incidents can be brought to the attention of Member States through the Commission or the High Representative also by a partner country or an international organisation. At policy level, the HWP ERCHT, chaired by the rotating Presidency, will play a central coordinating role in the preparation of Council decisions, thus enhancing internal coordination and helping develop a comprehensive and coherent EU approach to hybrid threats and campaigns, in accordance with established rules and procedures.

When HWP ERCHT is discussing a case, the EU INTCEN Hybrid Fusion Cell is invited to provide an intelligence assessment or briefing, if applicable. The Commission and the High Representative as well as Member States are also invited to contribute to this situational overview including by providing an update on the tools and measures put in place to counter the hybrid threats or campaign.

Member States can also invite the Commission services and the EEAS to provide them with possible options for reaction. This information should be given either in the form of an options paper or a verbal briefing, which should include information on the tools and instruments that are already in use or that could be employed in the particular case in accordance with their specific decision-making rules and procedures.



For measures that require a Council decision, existing decision-making procedures will apply. However, not all measures under this Framework will 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 in the case in hand in accordance with their specific decision-making rules and procedures.

In accordance with established rules and procedures and based on the scope and nature of the hybrid threat or campaign and the external actors in question, the Political and Security Committee (PSC) may also deliberate on the issue discussed within this Framework. Where the hybrid campaign is part of a crisis for which the Integrated Political Crisis Response (IPCR) arrangements have been activated, the IPCR procedural arrangements will apply. In accordance with its scope of competence and responsibilities, the HWP ERCHT, with guidance from Coreper and/or the PSC, will act as a preparatory body for the purpose of invoking the measures within this Framework that requires Council decisions.

Cooperation with relevant regional and thematic Council working groups is to be sought where relevant. Where the use of restrictive measures is concerned, the competent preparatory bodies within the Council, including the Foreign Relations (RELEX) Counsellors Working Party, will determine the next steps in accordance with their mandate. The Chair of the Council preparatory body from which the initiative or proposal to use restrictive measures originated ~~from~~, where appropriate in cooperation with the Chair(s) of the other preparatory Council bodies involved, including HWP ERCHT, may organise meetings and, where necessary, discuss the parameters of the initiative or proposal. The EEAS and the Commission services should provide assistance during the deliberations, including through the provision of proposals by the High Representative.

The decision to implement measures under the Framework should be accompanied by the political and legal context of the measures, including technical details where appropriate. In addition to the relevant provisions of the TEU and TFEU, this may include references to existing international law, voluntary non-binding norms of responsible state behaviour or any other applicable international agreement. Furthermore, the decision should set out the specific tasks in relation to the implementation of the measure. The decision on implementing measures should be taken at the appropriate level, to be defined on a case-by-case basis by the PSC, Coreper or the Council.

### Step-by-step process of activation and decision-making<sup>7</sup>:

In order to implement the EU Hybrid Toolbox, which brings together different instruments to detect and respond to a broad range of hybrid threats, as well as the FIMI Toolbox, the following step-by-step process on activation and decision-making applies:

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**,
2. **Member State(s)** request that the Council (e.g. through the HWP ERCHT) discuss the issue; as a part of this process, the **Commission** and the **High Representative** are invited to start preparations of possible options;
3. **Hybrid Fusion Cell** provides strategic foresight and comprehensive situational awareness, notably to assess the origin and features of the hybrid threats and campaigns; it can be complemented by other relevant EU institutions, bodies and agencies as well as CSDP missions and operations and international partners, including through open source information, where appropriate;
4. The **Commission** services and the **EEAS** as well as **Member States** can also be invited to contribute to the situational overview including by providing updates on their ongoing activities.
5. The **Commission services** and the **EEAS** issue proposals and recommendations, in an options paper where and when appropriate, and also provide timely information about measures taken within their scope of competence;
6. **Council** receives and discusses proposals and recommendations prepared by the Commission and the High Representative;
7. **HWP ERCHT** prepares recommendations and proposals for Coreper. If needed, the PSC may deliberate on the measures decided on within this Framework that fall within its mandate;
8. Depending on the nature of the measure proposed, the **Council** takes a decision on implementing a measure. On a case-by-case basis, the PSC may be involved.
9. **Member States**, the **High Representative** and the **Commission**, as the case may be, implement decisions;
10. **The Council** follows up on the implementation and relevant lessons learned. Such follow-up should include reporting by the relevant services of the Commission and the High Representative who are involved in the implementation of measures, cross-briefings (if other groups are also involved), and classified briefings by the Hybrid Fusion Cell if relevant as part of the follow-up;
11. **Member States** may request to revisit the relevant steps of the process should additional measures be required.

<sup>7</sup> The box is a simplified summary of the decision-making process. In terms of procedures, the text outside the box prevails.

### Attributing hybrid activities

Member States may propose coordinated attribution of hybrid activities, recognising that attribution remains a sovereign political decision of Member States based on all-source intelligence and taken on a case-by-case basis. Every Member State is free to make its own determination with respect to attribution of a hybrid campaign.

For the purpose of these implementing guidelines, it is important to distinguish between attribution as one of the tools of the EU Hybrid Toolbox ('political' or 'joint/coordinated<sup>2</sup> attribution) and attribution as a part of the decision-making process (technical attribution). The latter is based on intelligence (and open-source) assessment and done in order to take effective decisions. Dedicated support for technical attribution may be provided by the EU institutions, bodies and agencies and Member States.

When the perpetrator of a hybrid-campaign can be identified with a high degree of certainty, asymmetric and proportionate measures in line with international law may be taken, on a case-by-case basis, subject to approval. Such measures include forms of diplomatic, political, military, economic or strategic communication to prevent or respond to a hybrid campaign, including in the event of malicious activities that are not classified as internationally unlawful acts but are considered unfriendly acts.<sup>8</sup> The comprehensive situational awareness may include elements useful for the process of attribution and therefore require particular attention. Attribution could be made, based on an analysis of technical data and all-source intelligence, including possible interests of the aggressor. The Hybrid Fusion Cell, in close cooperation, when necessary, with other relevant EU institutions, bodies and agencies, CSDP missions and operations as well as partners, plays a valuable role in this regard by sharing its analyses related to the context and the origin of a hybrid campaign in accordance with its mandate. Member States may employ different methods and procedures for attribution of hybrid campaigns and use different definitions and criteria for establishing a degree of certainty on attributing a hybrid campaign. This framework does not attempt to harmonise those methods, procedures, definitions and criteria since attribution is a sovereign decision.

---

<sup>8</sup> Council conclusions on a Framework for a coordinated EU response to hybrid campaigns (ST 10016/22).

However, in order for a joint EU diplomatic response to be effective, the mechanism in this Framework aims to facilitate the decision-making process, including the process for collectively assessing the information provided and designing and implementing a measure, or a coherent approach including several measures, based on a comprehensive situational awareness and intelligence assessment on the origin of a hybrid campaign, when necessary.

Member States can ensure an effective coordinated EU response to hybrid campaigns by sharing relevant information through the Hybrid Fusion Cell and, as and where appropriate, through other mechanisms within the relevant constituencies, or by providing their assessment on particular aspects of a hybrid campaign to the appropriate preparatory body. It must be noted that there is no international legal obligation to reveal evidence on which attribution is based prior to an appropriate response, although it is recognised for the purposes of this Framework that Member States may choose to share such evidence, for instance in order to give effect to a joint EU diplomatic response or to convince other Member States to join them in a response to a hybrid campaign. Not all of the measures presented in this Framework will require attribution, but may be a means of preventing or mitigating a hybrid campaign, expressing concerns and signaling them in another way. Furthermore, the use of the measures under the Framework can be tailored to the degree of certainty that can be established in a particular case. When coordinated attribution is not possible or public attribution is not in the best interests of the EU and its Member States, well-calibrated asymmetric actions could also be envisaged on a case-by-case basis, subject to approval.

### **Role of the Integrated Political Crisis Response mechanism**

In situations where a hybrid campaign develops into a major, complex crisis which in turn leads to the activation of the IPCR, or where a hybrid campaign is part of a crisis for which IPCR has already been activated, the following procedure applies for invoking the measures under the Framework:

- In case of a crisis for which the IPCR arrangements<sup>9</sup> have been activated in full mode, following the appropriate agreed procedures<sup>10</sup> to handle the crisis at EU level, measures within this Framework could be part of the EU response at the political level. In this case, the IPCR procedural arrangements will apply. The IPCR arrangements are designed to allow a timely policy coordination and response at the EU political level (Coreper/Council) in the

---

<sup>9</sup> Council document 1078/13.

<sup>10</sup> EU operational protocol for countering hybrid threats ('EU Playbook').

event of major emergencies or crises. Specific expertise of the HWP ERC HT might be provided, if asked for, to support the IPCR.

- The IPCR is also used to coordinate the response to invocation of the solidarity clause (Article 222 TFEU) in order to ensure the coherence and complementarity of Union and Member State action at the strategic/political level. The arrangements for the implementation of the solidarity clause by the Union are defined by Council Decision 2014/415/EU<sup>10</sup>.

#### **IV. Categories of measures**

As the distinction between internal and external threats is becoming increasingly blurred by actors using hybrid tactics, a comprehensive and coordinated response to hybrid threats and campaigns should mobilise all relevant internal, and external EU policies and tools, and include all relevant civilian and military tools and measures. The individual categories presented below contain an open-ended and non-exhaustive set of possible measures and tools, which may require updating based on needs and developments in accordance with the key principles of maintaining efficiency, flexibility and the case-by-case approach. Some of the measures are cross-cutting and may be classified in several categories. Existing and new mechanisms and tools should be taken into account, including both the external and internal dimensions as appropriate.

Following the Council Conclusions of 21 June 2022, the measures in the EU Hybrid Toolbox have been organised in the following categories: preventive, cooperative, stability, restrictive and recovery measures and strengthening of solidarity and mutual assistance. Priority should be given to measures aiming to mitigate and terminate the impact of a detected campaign at the earliest stage possible, as well as to preventing its further expansion and escalation, discouraging its perpetrator from conducting further action and facilitating quick recovery.

The measures could be used either independently, sequentially or in parallel as part of a coherent strategic approach at EU level designed and implemented so as to influence a specific actor, and should take into account the broader context of EU external relations and the wider EU approach that aims to contribute to the mitigation of hybrid threats, conflict prevention and greater stability in international relations.

The Commission and the High Representative should mobilise all the EU's relevant tools and instruments, drawing on external and internal policies, in accordance with their respective rules and governance. Possible measures under the competence of the Commission could be considered, based on the existing mapping of general and sectoral measures at EU level<sup>11</sup> and the 2022 inventory of EU crisis management capabilities<sup>12</sup>, thus mobilising a broad range of relevant areas and tools while taking into account their autonomous nature, due to their legal basis and the associated decision-making mechanisms, and focusing on their potential to contribute to coordinated EU responses to hybrid threats and campaigns.

### **1. Preventive measures**

- Preventive measures implemented under the Framework include a wide range of measures for raising awareness; increasing resilience, capacity and confidence building, regular exercises and training; and including inter alia: EU-led capacity building efforts that can further support partners with strengthening their resilience to hybrid threats.
- EU CSDP missions and operations as an important tool at the EU disposal could make a contribution, in line with their mandates, by building the resilience of their host states through assisting, advising, and enhancing the capabilities of partners to withstand hybrid threats, while increasing overall EU situational awareness on hybrid threats by providing relevant information to the Hybrid Fusion Cell<sup>13</sup>.
- Developing a leading role for the EU as a normative power in countering hybrid threats in key domains such as information, cyber and economy.

### **2. Cooperative measures**

- Increased diplomatic engagement and cooperation with like-minded partners and countries, including EU partners in neighbourhood regions and beyond could take the form of dedicated dialogues, information sharing, exchange of best practices and increased coordination on response options and building solidarity.

---

<sup>11</sup> JOINT STAFF WORKING DOCUMENT Mapping of measures related to enhancing resilience and countering hybrid threats, SWD(2020) 152 final.

<sup>12</sup> Inventory of EU crisis management capabilities, European Commission, May 2022.

<sup>13</sup> In line with the Council conclusions on strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic, with the mini-concept on hybrid threats and the Guidance on countering hybrid threats in CSDP military operations and missions.

- Cooperation with NATO as a key strategic partner, in accordance with the joint EU and NATO declarations on EU-NATO cooperation and agreed actions for implementation, including situational awareness, information exchange, parallel and coordinated analysis of hybrid threats, strategic communication, countering FIMI, including disinformation, resilience building, training and exercises as well as coordinated responses to hybrid threats and cyber-attacks, on a case-by-case basis and in full respect of the principles of transparency, reciprocity and inclusiveness, as well as the decision-making autonomy and procedures of both organisations.
- Cooperation with other relevant international organisations and like-minded partners and countries, including in the UN and the G7, as well as with civil society and the private sector, in countering hybrid threats, with a view to securing a leading role for the EU in international norm development for countering hybrid threats.
- The future EU Hybrid Rapid Response Teams (HRRTs) should serve as one of the key instruments of the EU Hybrid Toolbox to support EU Member States and partner countries in countering hybrid threats, and supporting civilian and military CSDP missions and operations when they are the target for hybrid activities.
- Coordinated actions in countering malign foreign intelligence activities while this remaining predominantly a national competence of Member States.

### **3. Stability measures**

- Diplomatic engagement in the form of diplomatic démarches<sup>14</sup>, political declarations and statements at EU level<sup>15</sup> (by the High Representative on behalf of the EU/ HRVP statements/ spokesperson statements/ local EU statements), political and thematic dialogues, EU Council conclusions and other tools that have a signaling function and underline the unity and determination of the EU and its Member States in promoting de-escalation and facilitating peaceful resolution.
- These measures can be pursued in coordination with relevant international organisations, such as NATO and the UN,- and with like-minded partners and countries.

---

<sup>14</sup> In line with EEAS Guidelines for EU Political Démarches.

<sup>15</sup> In line with EEAS Guidelines on Statements and Declarations.



- CSDP missions and operations, when conditions are met and in line with their mandate, could make an important contribution by assisting, advising, detecting and enhancing the capabilities of partners to withstand hybrid threats as well as being able to detect and respond to hybrid threats. Options for civilian CSDP missions are further explained in the Mini-concept on civilian CSDP support for countering hybrid threats.
- HRRTs adaptable to threats 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 with countering hybrid threats.
- Strategic communication (including tailor-made public statements and political declarations) with clear, strong, proactive and consistent messaging accompanying EU responses to hybrid threats, preferably coordinated with the EU institutions, Member States and partner countries and organisations, could reinforce their impact and shape the perception of the EU's intent.

#### **4. Restrictive measures**

- While public attribution remains a sovereign national prerogative, coordinated attribution of hybrid activities at EU level could be considered on a case-by-case basis and be accompanied by strategic communication and a diplomatic response to highlight Member States' determination to hold the perpetrator accountable.
- The EU may impose restrictive measures<sup>16</sup> against third countries, entities or individuals on the basis of a Council decision adopted under Article 29 TEU coupled with a Council regulation setting out the measures needed to make it operational, adopted under Article 215 TFEU. If necessary, the EU may impose restrictive measures, adopted under the relevant provisions of the Treaties, in response to hybrid activities. The imposition of restrictive measures must be done in accordance with the relevant procedures agreed by Member States and set out in the guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy. Such measures can include, inter alia, travel bans, arms embargos, freezing funds or economic resources. The EU can also impose sectoral measures, such as economic and financial measures.

---

<sup>16</sup> Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy (5664/18).



- Exploring the possibility of creating new EU restrictive measures to address hybrid activities could be considered. The Council can also deliberate about complementing existing sanctions regimes where necessary and based on prior legal analysis.<sup>17</sup>
- The continued implementation of the EU Cyber Diplomacy Toolbox will be an important step to prevent, discourage, deter and respond to malicious cyber activities that are part of a hybrid campaign.

## **5. Recovery measures**

- Specific recovery measures could be considered to address disruption in domains immediately and reduce its impact, thereby leading to greater preparedness, reduced vulnerability or the prevention of future hybrid activities.

## **6. Strengthening solidarity and mutual assistance**

- The measures within this Framework could be used to support or complement legal responses by Member States. The EU could, at the request of one or more Member State(s), provide support to Member States that individually or collectively resort to responses in accordance with international law that are not available within the CFSP. Such responses may take the form of any lawful measure, ranging from diplomatic steps, to stronger individual or cooperative measures.
- When a Member State is the victim of a hybrid attack that constitutes an internationally wrongful act, it may legally resort to proportionate countermeasures. These countermeasures constitute actions directed at another State that is responsible for the internationally wrongful act, which would otherwise violate an obligation owed to that State. Such countermeasures are conducted to compel or convince the latter to cease the malicious hybrid activity, in compliance with its international obligations.
- In grave instances, serious hybrid campaigns could amount to a use of force or an armed attack within the meaning of the Charter of the United Nations. In the latter case, Member States may choose to exercise their inherent right of individual or collective self-defence as recognised in Article 51 of the Charter of the United Nations and in accordance with international law, including international humanitarian law. Member States may propose coordinated attribution of hybrid activities, while recognising that attribution is a sovereign national prerogative. A Member State may also choose to invoke the solidarity clause

---

<sup>17</sup> Ibid.

(Article 222 TFEU)<sup>18</sup> and/or the mutual assistance clause (Article 42(7) TEU) to call on other Member States to provide aid and assistance. This shall not prejudice the specific character of the security and defence policy of certain Member States. Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organization, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation. EU institutions could be called upon to support, through coordination, and/or to facilitate activities of Member States undertaken in the context of the implementation of Article 42(7) TEU, if so requested by Member States.

---

---

<sup>18</sup> In line with Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause (2014/415/EU).