EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 5.7.2016
SWD(2016) 227 final

JOINT STAFF WORKING DOCUMENT

EU operational protocol for countering hybrid threats

'EU Playbook'

1. Purpose

This document is prepared in order to implement Action 19 of the Joint Framework on countering Hybrid Threats, which foresees a " common operational protocol between Member States, the Commission and the High Representative is to outline effective procedures to follow in case of a hybrid threat, from the initial identification phase to the final phase of the attack, and mapping the role of each Union institution and actor in the process."[1]

To maximise effectiveness, economies and efficiencies, this common operational protocol:

- Builds on existing crisis management arrangements at EU level[2].
- Provides for the integration of the EU Hybrid Fusion Cell into these arrangements.

This protocol outlines the modalities for:

- coordination,
- intelligence fusion and analysis,
- informing policy recommendations and decision-making within existing structures,
- exercises and training, and
- cooperation with partner organisations, including the North Atlantic Treaty Organisation (NATO).

All activities explained in this protocol are:

- in full compliance with the applicable rules on security and exchange of classified information[3] of all actors involved. For exchange of classified information, available accredited tools shall be used[4];
- having due regard to non-binding instruments (Memorandums of Understanding (MoUs) or Administrative arrangements)

---

1 Joint Communication to the European Parliament and the Council JOIN(2016) 18 of 6.4.2016, Joint Framework on countering hybrid threats – a European Union response.

2 The common operational protocol builds on existing sector-specific mechanisms or arrangements (led by Commission services, the EEAS or EU Agencies). It does not replace them nor infringe on existing competencies.

3 Commission Decisions on Security in the Commission 2015/443 of 13.03.2015 and on Rules for Protecting EU Classified Information 2015/444 of 13.03.2015; High Representative Decision on the security rules for the European External Action Service 2013/C 190/01 of 19.04.2013; Council Decision on the Security Rules for Protecting EU Classified Information, 2013/488/EU - OJ L 274 of 15.10.2013, p 1

4 In June 2016, these transmission channels include CIMS (Classified Information Management System), ACID (encryption algorithm), RUE (secure system to create, exchange and store RESTREINT UE / EU RESTRICTED documents) and SOLAN

2. Key terms (in alphabetical order)

ARGUS: ARGUS is the Commission's general alert system in place since 2005[6]. It is a process supported by an information technology (IT) tool and a dedicated network of 24/7 duty officers in each relevant Directorate-General. ARGUS foresees two phases, Phase I (information sharing during early phase or modest crisis) and Phase II (crisis coordination meetings to address a major multi-sectoral crisis).

CERT-EU: the Computer Emergency Response Team of the EU institutions, bodies and agencies. Its mandate is to improve the protection of the EU institutions, bodies and agencies against cyber threats. It is part of the EU CSIRT[7] network linking all Member States' national CSIRT and exchanging operational information about cyber threats. CERT-EU has technical agreements on cyber threats with NATO CIRC[8] and all major IT vendors.

EEAS CRM: The European External Action Service (EEAS) Crisis Response Mechanism (CRM)[9] is a system for responding in a coordinated and synergic way to crises and emergencies of external nature or having an external dimension, including hybrid threats. The system is composed of arrangements and structures and is triggered by any events potentially or actually seriously impacting EU's or any Member States' security interests.

ERCC: The Emergency Response Coordination Centre in the Commission (Directorate-General for European Civil Protection and Humanitarian Aid Operations - DG ECHO)) supports and coordinates a wide range of prevention, preparedness and response activities. Inaugurated in 2013, it acts as the hub of the Commission's crisis response (liaising with other EU crisis rooms) and as the central IPCR 24/7 contact point.

EU SITROOM: The EU Situation Room is part of the EU Intelligence and Situation Centre (EU INTCEN) and provides the EEAS with operational capacity to ensure an immediate and effective response to crises. It is the EU permanent civilian-military stand-by body that provides worldwide monitoring and situation awareness with a 24/7 capacity/capacity.

EU Hybrid Fusion Cell: The EU Hybrid Fusion Cell offers a single focus for the analysis of hybrid threats within the EU Intelligence and Situation Centre (EU INTCEN) of the EEAS.[10] Its mandate and tasks will be defined in its Terms of Reference. The EU Hybrid Fusion Cell receives analyses and shares classified and open source information specifically relating to indicators and warnings concerning hybrid threats from different stakeholders within the EEAS (including EU delegations), Commission services, EU agencies and Member States. In

---

5 Commission Decision 2006/25/EC and COM(2005)662 of 23.12.2015

6 Commission Decision of 23 December 2005 amending its internal Rules of Procedure (2006/25/EC, Euratom)

7 Computer Security Incident Response Team

8 Computer Incident Response Capability

9 CRM is currently (June 2016) being finalised.

10 The EU Hybrid Fusion Cell will function in accordance with its Terms of Reference which are under preparation.

liaison with existing similar bodies at EU and at national level, the Fusion Cell analyses external aspects of hybrid threats affecting the EU and its neighbourhood.

Hybrid threats[11]**:** Hybrid threats can be characterised as a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological, information), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of open organised hostilities. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity with the intention to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats.

IPCR: The Integrated Political Crisis Response (IPCR) Arrangements are crisis arrangements agreed in 2013 by the Council[12] for "major emergencies or crises, inside or outside the EU, of such wide-ranging impact or political significance that require timely policy coordination and response at EU political level". IPCR Standard Operating Procedures (SOPs)[13] explain in detail the working modalities of IPCR which include i.a. two activation modes: "information sharing" and "full activation". IPCR is also activated in case of invocation of the Solidarity Clause (Article 222 TFEU).[14] IPCR is supported by an ISAA capability (for ISAA see below) and by a central 24/7 PoC in the ERCC.

ISAA: The Integrated Situational Awareness and Analysis (ISAA) is a capability developed by the Commission and EEAS within their respective roles and responsibilities to support decision making in IPCR. ISAA builds also on information and analysis provided by Member States and EU Agencies. Working arrangements are detailed in the ISAA Standard Operating Procedures[15]. ISAA reports are prepared under the leadership of the most relevant service in the Commission or EEAS for the given crisis, following the "centre of gravity" approach.

ISG "Countering Hybrid Threats (CHT)": The Inter-Service Group (ISG) on countering hybrid threats ensures a comprehensive approach and monitors progress on actions foreseen in JOIN(2016)18. It is co-chaired by representatives of the EEAS and the Commission services at Director General /Deputy Secretary-General level and meets quarterly. For more information, see section 4 below.

ISG "C3M": The "Community Capacity in Crisis Management (C3M)" inter-service group network is a network that exists since 2008, bringing together regularly all Commission services and EU agencies involved in crisis management to increase awareness raising,

---

[11] Definition used in JOIN(2016) 18 of 6.4.2016 – see also footnote 1

[12] 10708/13 on the "Finalisation of the CCA Review process: the EU Integrated Political Crisis Response Arrangements", approved by the Council on 24 June 2013.

[13] 12607/15 "IPCR Standard Operating Procedures", agreed by Friends of the Presidency group and noted by COREPER in October 2015

[14] Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause (2014/415/EU)

[15] DS 1570/15 of 22 October 2015

enhance synergies and exchange information. EEAS also attends. The ISG acts as the human network of points of contact from all operational crisis rooms / situation centres.

Points of Contact for EU Hybrid Network: The EU Internal Points of Contact are personnel nominated to represent their Directorate-General, service or agency on hybrid related matters. In line with the Joint Communication on *Countering Hybrid Threats*, Member States are invited to nominate dedicated national points of contact for secure inter-action with the EU Hybrid Fusion Cell. The virtual hybrid network includes EU points of contact, as well as the points of contact nominated by Member States. These Points of Contact should hold the appropriate security clearances to permit access to routine reporting from the EU Hybrid Fusion Cell up to the classification level SECRET UE / EU SECRET.

Standard Operating Procedures (SOPs): a set of step-by-step instructions for carrying out routine operations. Their purpose is to achieve efficiency, quality output and uniformity of performance, while reducing miscommunication and failure to comply with internal rules and procedures.

STAR: The Strategic Analysis and Response centre is part of the Commission (Directorate-General for Migration and Home Affairs - DG HOME). STAR provides information and assessment, in particular risk analysis, to support policy formulation as well as support crisis management situation awareness and communication needs. Its crisis room is located in a resilient and highly secure facility allowing for the handling and exchange of classified information with Commission services, EEAS and relevant Agencies (notably Europol and Frontex).

3. The EU Hybrid Fusion Cell

The EU Hybrid Fusion Cell is the designated focal point for intelligence relating to potential hybrid threats.

The Director of INTCEN, as senior official responsible for the Fusion Cell, is tasked to rapidly analyse relevant incidents and inform the EU's strategic decision-making processes, including by providing inputs to the security risk assessments carried out at EU level.

Reports of special interest are to be forwarded in the first instance by the Director of INTCEN to the entry points at the operational or policy level as appropriate according to established procedures in each organisation. Routine reports should be distributed to the Hybrid Network with a quarterly summary presented to the CHT and C3M ISGs.

The EU Hybrid Fusion Cell's analytical output will be processed and handled in accordance with the EU classified information and data protection rules and the agreed Terms of Reference. The Head of the Fusion Cell will liaise with Commission services and other existing bodies at EU and national level. Member States should establish National Contact Points connected to the EU Hybrid Fusion Cell.

The Director of INTCEN is named as the responsible person for the compilation of products related to Hybrid threats and the subsequent analysis reports.

For information in particular on cyber threats, the Hybrid Fusion Cell cooperates closely with CERT-EU, benefiting from its network of peers and partners.

4. Crisis management procedures in the EU

In the EU, coordination of crisis management occurs at three levels: political, operational and technical. It addresses the full crisis management cycle: prevention/mitigation, preparedness, response, recovery.

Dedicated procedures govern the implementation of the Commission (ARGUS), the Council arrangements (IPCR) and the EEAS Crisis Response Mechanism (CRM). Within the CRM, identified points of entry allow coordination with EU actors and international partners.

When there is the need for wider / emergency consultation on hybrid threats among Commission services, EEAS and EU agencies, appropriate use is made of these crisis management procedures.. For an indicative overview of these procedures[16], see Diagram 1.

[16] For detailed information on these procedures, please refer to the Standard Operating Procedures of IPCR, ARGUS and CRM.

Diagram 1: Indicative Coordination levels in EU Crisis Management procedures[17]

At the **political strategic level**, the points of entry for activation and coordination of the relevant crisis procedures are:

- For the European Council, the President.
- For the Council, the rotating Presidency (Head of State or Minister in charge).
- For the European Commission, the President or the delegated Vice-President / Commissioner.
- The High Representative of the Union for Foreign Affairs Security Policy / Vice-President of the Commission.

At the **operational level**, the points of entry are:

- For the Council, the Presidency (Chair of COREPER II).
- For the Commission services, the (Deputy) Secretary General.
- For the EEAS, the (Deputy) Secretary General for Crisis Response and CSDP.

At the **technical level**, the points of entry are:

- For the Council, the Secretariat General (IPCR Secretariat).
- For the Commission: the Secretariat General (ARGUS secretariat), the ERCC (24/7 operational service), and the designated lead service (depending on the nature of the crisis).
- For the EEAS, EU Situation Room and the nominated geographic or thematic service.
- For the EU agencies, the respective parent DG in the Commission or the EEAS (first point of contact).

5. Triggering existing EU Crisis Management Arrangements for a hybrid threat

In the event of hybrid threat, existing procedures are used to ensure that the early warning or initial indication of a threat as identified by the EU Hybrid Fusion Cell can be addressed before a full blown crisis occurs.

When the relevant EU actors decide to activate their respective crisis arrangements (IPCR, ARGUS, CRM), interaction between the technical and operational levels is based on the use of the respective Standard Operating Procedures. This ensures that political decisions can be informed by situational awareness and evidence based analysis provided by the technical level to the operational level and then to the political level. The hybrid network is an integral part of this process using the EU Hybrid Fusion Cell as its information analysis hub. The specific process before and during the emergency phase is described below.

[17] At present, the EEAS is not formally part of the ARGUS process, but EEAS attends the ARGUS Phase II Crisis coordination meetings with the HRVP Cabinet.

5.1 Pre-crisis phase

Given the nature of hybrid threats whose purpose and design is often to stay below the threshold of activity that might trigger a recognisable crisis, the EU may need to take appropriate action in the pre-crisis phase.

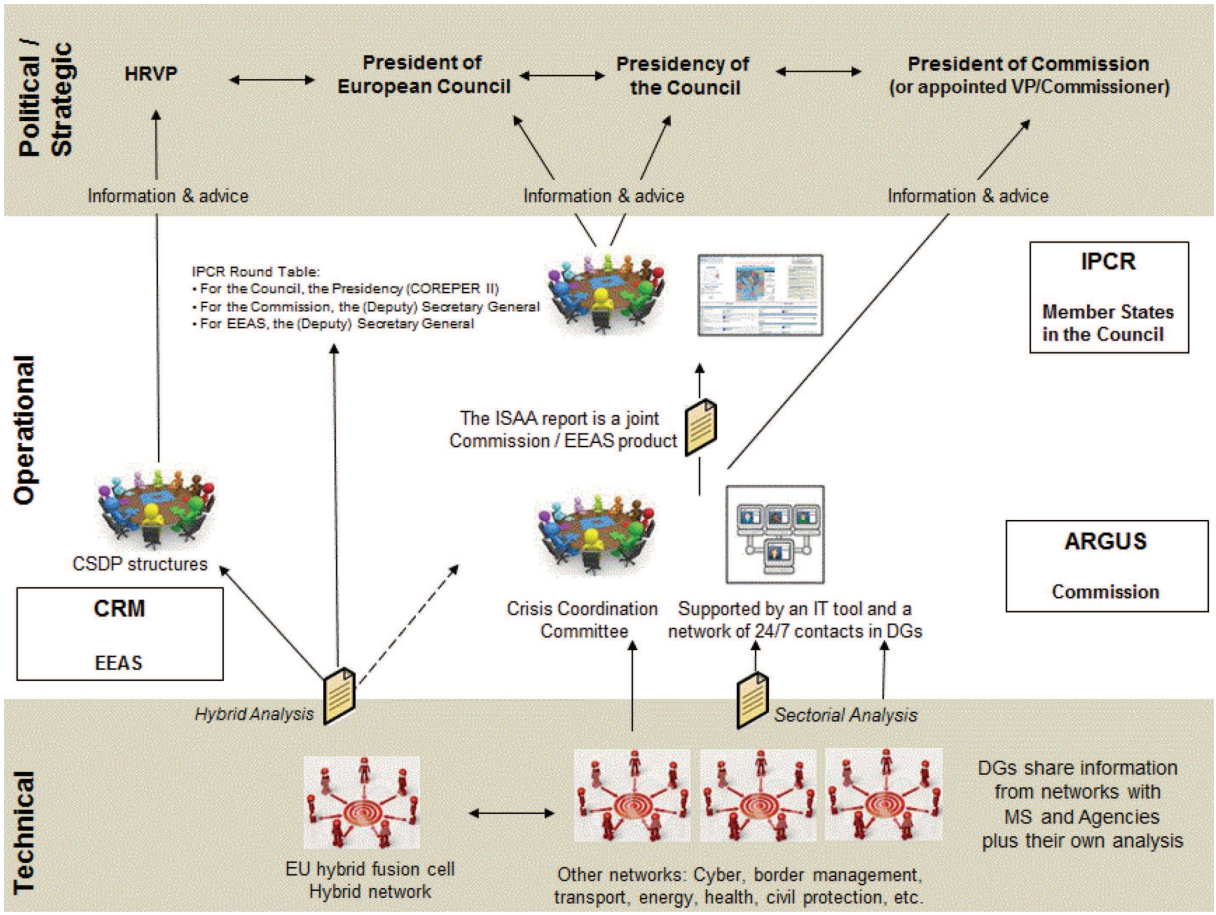

Diagram 2: Information Flow in case of a hybrid threat

Preparedness

As outlined in Section 3, the Fusion Cell is tasked to rapidly analyse relevant incidents and inform the appropriate coordination structures.

The regular reporting from the Fusion Cell can contribute to inform sectoral policy-making to enhance preparedness.

Rapid alert / early warning (eruption of a possible crisis)

Complementing the work of the Situation Room, the sectorial rapid alert / early warning systems and the intelligence provided by Member States, the EU Hybrid Fusion Cell provides early warning and situational awareness on potential hybrid threats affecting the EU and its partners.

Therefore, when the analysis of the EU Hybrid Fusion Cell report indicates the existence of possible hybrid threats directed against a Member State, partner countries or organisation, the Director of INTCEN will inform in the first instance to the operational level for urgent attention according to the established procedures.

The operational level will then prepare recommendations for the political strategic level, including the possible activation of crisis management arrangements in monitoring mode (e.g. IPCR monitoring page, ARGUS phase 1 event, CRM)..

5.2 During a major emergency

During an acute crisis, the point of entry during IPCR activation is the ERCC, as foreseen in IPCR procedures. In case of a major threat or attack, contacts will be made at the operational level in view of full activation of the relevant crisis procedures (IPCR, ARGUS, CRM). The ISAA lead service is determined in line with the IPCR SoPs.

The EU Hybrid Fusion Cell will support and provide contributions to the ISAA lead service and the IPCR Roundtable, as appropriate.

6. Training and Exercises

In order to support the protocol, EU staff (including those deployed to EU delegations, operations and missions) will be regularly trained to recognise early signs of hybrid threats.

The multi-annual EU Exercise Programme presented annually to the Council will systematically include exercises with *inter alia* hybrid scenarios. Making best use of facilities and expertise across EU institutions, these exercises will test the operational protocol and draw lessons drawn in order to identify gaps and opportunities for improvement.

Staff contacts with partners, specifically NATO, are particularly relevant in the hybrid context with a view to facilitating fully inclusive parallel and coordinated exercises.

7. Cooperation with NATO

In line with the 'Joint Communication on Countering Hybrid Threats' welcomed by the Council on 19 April 2016, the High Representative in coordination with the Commission, will operationalise EU-NATO cooperation in the four areas proposed under Action 22 of the Joint

Communication, based on the principle of inclusiveness, while respecting each organisation's decision-making autonomy and data protection rules. These areas are:

- situational awareness,
- strategic communications,
- cybersecurity, and
- crisis prevention and response.

Throughout the early warning and crisis management cycle, the EU interfaces identified at policy, operational and technical level (as presented in diagram 1), should interact with appropriate counterparts in NATO.[18]

The ongoing informal EU-NATO staff-to-staff dialogue on hybrid threats should be strengthened in order to synchronise the two organisations' parallel activities in the above areas.

The precise modalities of EU-NATO staff-to-staff dialogue will be elaborated in a subsequent document operationalising Action 22 of the Joint Communication on Countering Hybrid Threats.

[18] Based also on technical agreements such as the technical agreement between CERT-EU and NATO-CIRC for facilitating information exchange in case of cyber threats.