Council of the
European Union

Brussels, 20 April 2023
(OR. en)

8500/23

HYBRID 16
DISINFO 20
IPCR 26

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	20 April 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2023) 116 final
Subject:	JOINT STAFF WORKING DOCUMENT EU Protocol for countering hybrid threats

Delegations will find attached document SWD(2023) 116 final.

Encl.: SWD(2023) 116 final

EUROPEAN
COMMISSION

HIGH REPRESENTATIVE
OF THE UNION FOR
FOREIGN AFFAIRS AND
SECURITY POLICY

Brussels, 19.4.2023
SWD(2023) 116 final

JOINT STAFF WORKING DOCUMENT

EU Protocol for countering hybrid threats

Contents

1. Purpose

The purpose of the EU Protocol for countering hybrid threats is to outline processes and tools applicable in case of hybrid threats or campaigns throughout the whole crisis management cycle, starting from prevention, preparedness and initial identification to response, recovery and lessons learnt, and to map the roles of various EU institutions, bodies and services, building on the existing crisis management arrangements. In addition, it covers communication, as well as cooperation with external partners. This revised version of the Protocol takes into account developments since the previous version of 2016, including lessons from Parallel and Coordinated Exercises (PACE) and further deepening cooperation with NATO, as announced in the EU Security Union Strategy[1] and in line with the EU's Strategic Compass for Security and Defence[2].

What is a hybrid threat?

Hybrid threats can be characterized as a mixture of coercive and subversive activity, conventional and unconventional methods (e.g. diplomatic, military, economic, technological, cyber, 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 formally declared or actual warfare.[3] There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. The methods used include foreign information manipulation and interference, economic coercion, interference in democratic processes, disruption on essential sectors or critical infrastructures and instrumentalisation of migrants, amongst others.

Example 1: Russia's 'legal warfare' in Donbas (2014) and Ukraine (2022)

Legal warfare (or the use of legal means to support a political-military objective) is an integral part of Russia's hybrid strategy. Territories under Russian de-facto control such as Transnistria, South Ossetia and Abkhazia, have proved vulnerable to the effects of this approach. Legal warfare has been extensively used in the war in Donbas starting in 2014. Shortly after the invasion and illegal annexation of Crimea, Russian-backed armed formations instigated conflict in eastern Ukraine. Armed groups calling themselves 'self-defence units' seized and occupied administrative buildings, and finally officially declared the so-called 'People's Republics' of Donetsk and Luhansk in April 2014. Despite rejecting allegations of leading, fighting beside, training and supplying separatists, Moscow's disguised involvement was quickly understood as a strategy to exacerbate regional instability. The organisation of a sham referenda in May

[1] COM(2020) 605 final, 24 July 2020.

[2] https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

[3] For the purpose of theProtocol, the definition of hybrid threats is as in the EU's 'Joint Framework on Countering Hybrid Threats': *"While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare."* JOIN(2016) 18 final, 6 April 2016.

2014 was modelled on the earlier Crimean scenario and constituted a first step towards total political and administrative control over the territory. Similarly, Russia used sham referenda organised in occupied territories to justify the attempted illegal annexation of four regions of Ukraine in 2022.

Example 2: COVID-related disinformation on vaccination (2020)

Disinformation campaigns are widely perceived as a threat to democratic processes. Many reports of foreign interference in the 2016 Brexit referendum or the 2017 French presidential elections have highlighted the EU's vulnerabilities. More recently, the COVID-19 pandemic, also accompanied by an 'infodemic' as highlighted by the World Health Organisation, renewed discussions around responses to intentional information manipulation and disinformation. Indeed, intentional information manipulation and disinformation, combined with the significant amplification of misinformation, have created a continuing climate of distrust and confusion in many European countries. Russian and Chinese information manipulation and interference strategies targeted the vaccination campaign in particular, aiming at undermining public trust in national public health systems and the EU's action to protect the lives of citizens.

Policy development fora

The main EU fora to discuss and develop the EU policy on countering hybrid threats are:

Interservice Group on Countering Hybrid Threats – a policy coordination group designated to ensure a comprehensive whole-of-government approach and monitor progress of actions. The group is co-chaired by representatives of the Commission services and the EEAS and meets when needed. In order to ensure that hybrid threats considerations are mainstreamed into policymaking, the Interservice Group has developed a network of points of contact among the different Commission services and the EEAS.

Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats[4] of the Council of the EU facilitates coordination and policy responses to hybrid threats. This includes countering foreign information manipulation and interference as well as sharing best practices to bolster awareness and resilience of the EU and its Member States and to ensure that there are no overlaps or gaps in these fields. It was established in 2019 and is chaired by the rotating Presidency of the Council.

Interservice group 'Community Capacity in Crisis Management' ('C3M') is a network of crisis management practitioners that since 2008 regularly brings together colleagues across the Commission services, EEAS, EU Agencies, as well as the General Secretariat of the Council to increase awareness, exchange views and enhance synergies during a crisis.[5] It acts both as an internal 'think tank' and contributes to crisis management policy development across the EU Institutions, including on issues related to hybrid threats.

[4] https://www.consilium.europa.eu/en/council-eu/preparatory-bodies/horizontal-working-party-on-enhancing-resilience-and-countering-hybrid-threats/.

[5] The network includes more than 20 Commission services and 10 EU Agencies.

2. Framework for a coordinated EU response to hybrid campaigns

The Strategic Compass for Security and Defence called for the development of the **EU Hybrid Toolbox**, bringing together different instruments to detect and respond to a broad range of hybrid threats. In its conclusions of 21 June 2022[6], the Council introduced a **framework for a coordinated response to hybrid campaigns** (Framework) affecting the EU, Member States and partners, which should also be used to address foreign information manipulation and interference (FIMI). The Framework is aimed at facilitating a comprehensive response to hybrid threats and campaigns by mobilising all relevant internal and external EU policies and tools, as set out in the EU Security Union Strategy 2020-2025, and include all relevant civil and military tools and measures. The implementing guidelines for the Framework set out steps leading to coordinated response to hybrid campaigns and preparatory practices. 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.[7]

3. Resilience and prevention

The European Council conclusions of December 2021 recognise that a broad range of EU actions contribute to the EU's resilience against hybrid threats.[8] The adoption of legislative and policy measures at EU level has the advantage of providing a coordinated regulatory and policy framework, which is essential to enhance resilience. Through these measures, the EU and its Member States define the obligations of authorities, institutions and economic operators and steer support and cooperation measures in and across critical sectors, including energy, transport, space or digital. Hybrid considerations are mainstreamed in policy-making by including hybrid threats in the Better Regulation toolbox as one of the key impacts to be assessed when preparing new policy initiatives.

A number of initiatives have been taken at EU level to facilitate and support Member States' cooperation, develop policy solutions, support capacity building and innovation, and enable the sharing of best practices. This includes the identification of sectoral resilience baselines, as well as domain-specific measures, such as the Cyber Diplomacy Toolbox[9] and the FIMI Toolbox[10].

[6] Council Conclusions on a Framework for a coordinated EU response to hybrid campaigns, 21 June 2022

[7] Implementing Guidelines for the Framework for a coordinated EU response to hybrid campaigns, 14 December 2022 (15880/22).

[8] European Council conclusions of December 2021, Council conclusions on enhancing preparedness, response capability and resilience to future crises, November 2021 (14276/21).

[9] Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), 19 June 2017 (10474/17).

[10] Council conclusions on Foreign Information Manipulation and Interference (FIMI), 18 July 2022 (11429/22).

The broad range of EU instruments that can be engaged to face hybrid threats - although not designed with this specific purpose in mind - are listed in the Inventory of EU crisis management capabilities[11].

4. Preparedness

We should raise the awareness of EU staff (including colleagues in EU delegations, CSDP missions and operations), to recognize early signs of hybrid threats, act on them effectively, by encouraging participation in existing training programs and conducting targeted practical exercises.

Training

The European Centre of Excellence for Countering Hybrid Threats (HCoE) has started organising training courses on hybrid threats, in addition to organising table-top exercises and policy-based discussions. The main objective is to provide the training audience (practitioners from interested authorities of its Participating States as well as NATO and the EU institutions) with the basis for an analytical approach to hybrid threats. Hybrid Points of Contact of the Commission services and the EEAS have participated in these courses. The European Security and Defence College (ESDC)[12] also has a specific training course on hybrid threats.

The Commission has also started training courses for EU staff on crisis management and crisis communication. Although these training courses do not specifically focus on hybrid threats, they can be used to increase sensitivity by also covering hybrid scenarios.

Exercises

The European Union Programme of Exercises and Exercise-Related Activities under the CFSP 2023-2027[13] and the multi-annual Exercise Programmes of the Commission[14] are compiled annually and include also exercises with hybrid scenarios. This includes Parallel and Coordinated Exercises (PACE) with NATO that, after the pilot phase in 2017-18, have been extended until 2023. PACE exercises are designed to cover a broad range of areas and simulate a severe hybrid attack, thus testing the resilience and preparedness of the Member States and EU institutions.

The Commission's crisis management exercise policy – which also covers the EU Agencies – is under preparation.

[11] Document sg.g.3(2022)4866036. See also Hybrid Threats: A comprehensive resilience ecosystem, JRC 130097.
[12] Education & Training - ESDC (europa.eu).
[13] ST 6787/23
[14] ST 6803 2022 COR 1.

5. Detection, early warning and situational awareness

To be dealt with effectively and efficiently, hybrid threats need to be spotted long before they escalate into major crises. This requires preparedness, early detection, the capability to connect dots and alerting those who need to know, while at the same time filtering information from noise and presenting it fully, yet concisely, to decision-makers in a timely manner.[15]

With regard to hybrid threats, the EU Intelligence and Situation Centre (Intcen) **Hybrid Fusion Cell** (HFC), with the support of EUMS Intelligence Directorate under the Single Intelligence Analysis Capacity (SIAC), plays a central role in contributing to the decision-making process by providing EU institutions, bodies and agencies, as well as Member States with strategic, intelligence-based assessments on hybrid threats[16], including an annual Hybrid Trends Analysis[17].

The HFC reporting covers hybrid activities and strategic objectives of various state and non-state actors and their proxies, as well as key trends and events that might lead to an escalation of hybrid threats. Within existing limitations of classified information sharing, the HFC engages in analytical exchanges with partners, notably with the NATO Hybrid Analysis Branch and like-minded third countries.

[15] See inter alia 'The landscape of Hybrid Threats: A conceptual model' - JRC(123305).
[16] Including on the EU as a whole, Member States, EU Institutions, CSDP missions and operations and the EU's interests abroad.
[17] The HTA is based on voluntary contributions provided by relevant governmental, intelligence and security structures of the Member States, the EU Institutions and CSDP missions and operations.

Furthermore, instruments like the EEAS managed Rapid Alert System on Disinformation and the EUvsDisinfo project, as well as developing new ones within the EEAS such as an Information Sharing and Analysis Center for FIMI will contribute to early warning, situational awareness, and tackling hybrid threats. To reduce exposure to such threats, the Commission services and EEAS will also continue to strengthen the monitoring and analysis of media and social media and continue to expose the malign behaviour of hybrid actors. Eurobarometer surveys of public opinion trends will continue to help to provide a mapping of the media landscape and allow EU decision-makers to detect trends and feed into building resilience.

6. Crisis coordination

In case of escalation into a (major) crisis, a complex system of crisis coordination arrangements across the EU institutions and bodies springs into action.

The main high-level arrangements for coordination of a multi-sectoral crisis are ARGUS in the Commission, the Integrated Political Crisis Response (IPCR) arrangements in the Council, and the EEAS Crisis Response Mechanism (CRM), which interact in various ways. This ensures that political decisions are informed by integrated situational awareness and evidence-based analysis, and good coordination amongst a range of sectoral measures.

ARGUS is the Commission's high-level crisis coordination system established in 2005.[18] It is a process supported by a network across the Commission services, as well as an eponymous rapid alert IT system also accessible to the EEAS and EU agencies. ARGUS has two phases: Phase I (information sharing during early phase or smaller-scale crisis, which is activated and led by the most affected service and facilitated by the ERCC); Phase II can be activated by the Commission President and triggers multi-sectoral coordination involving all relevant EU services, as well as the Cabinets in the Crisis Coordination Committee (CCC). Examples of the latter are the Russian aggression against Ukraine (2022), COVID-19 (2020), the migration/refugee crisis (2015), volcanic eruption in Iceland (2011), Fukushima triple disaster (2010), and the threat of H1N1 pandemic (2009).

Integrated Political Crisis Response (IPCR) arrangements in the Council were developed in 2013[19] to deal with major emergencies or cross-sectoral crises. The arrangements are led by the rotating Presidency of the Council, with the input of the Commission services and the EEAS. They have two activation modes: 'information sharing' and 'full activation' that are activated by the Council Presidency. IPCR arrangements are also activated automatically in case of invocation of the Solidarity Clause (Article 222 TFEU) by a Member State. In case of activation, Integrated Situational Awareness and Analysis (ISAA) reports are produced by the Commission services and the EEAS on the basis of the Presidency guidelines; the full activation implies convocation of informal roundtables with the participation of affected Member States, EU institutions and other relevant stakeholders. Thus far, there were three full activations of the IPCR arrangements: the war in Ukraine (2022), the COVID-19 pandemic (2020) and the migration/refugee crisis (2015).[20]

The EEAS **Crisis Response Mechanism (CRM)**, managed by the EEAS Crisis Response Centre (EEAS CRC) contains the arrangements to ensure a coordinated and timely response to external crises and emergencies with a potential or actual impact on the security interests of the EU, particularly in the context of the duty of care for the safety of EU staff and support to Member States in case of a consular crisis. As part of the CRM, Crisis Meetings can be organised to ensure a shared situational awareness and the exchange of relevant information between senior managers from the EEAS, Commission services and the Council, while the aim of a Crisis Cell is to ensure 24/7 monitoring of an evolving, sensitive situation with a potential impact on the security of staff posted in EU Delegations, and in case of risk of a consular crisis.

The EU crisis response is operationalized by the following 24/7 structures:

[18] Commission Decision 2006/25/EC of 23.12.2005.
[19] 10708/13 on the 'Finalisation of the CCA Review process: the EU Integrated Political Crisis Response Arrangements'.
[20] Following the European Council conclusions of 16 December 2021 the discussion is within the ad hoc working party on preparedness, response capability and crisis response to future crisis, established in 12 January 2022, as to how to strengthen the structures, including IPCR, that allow the EU to prepare for crises and to respond effectively when they occur.

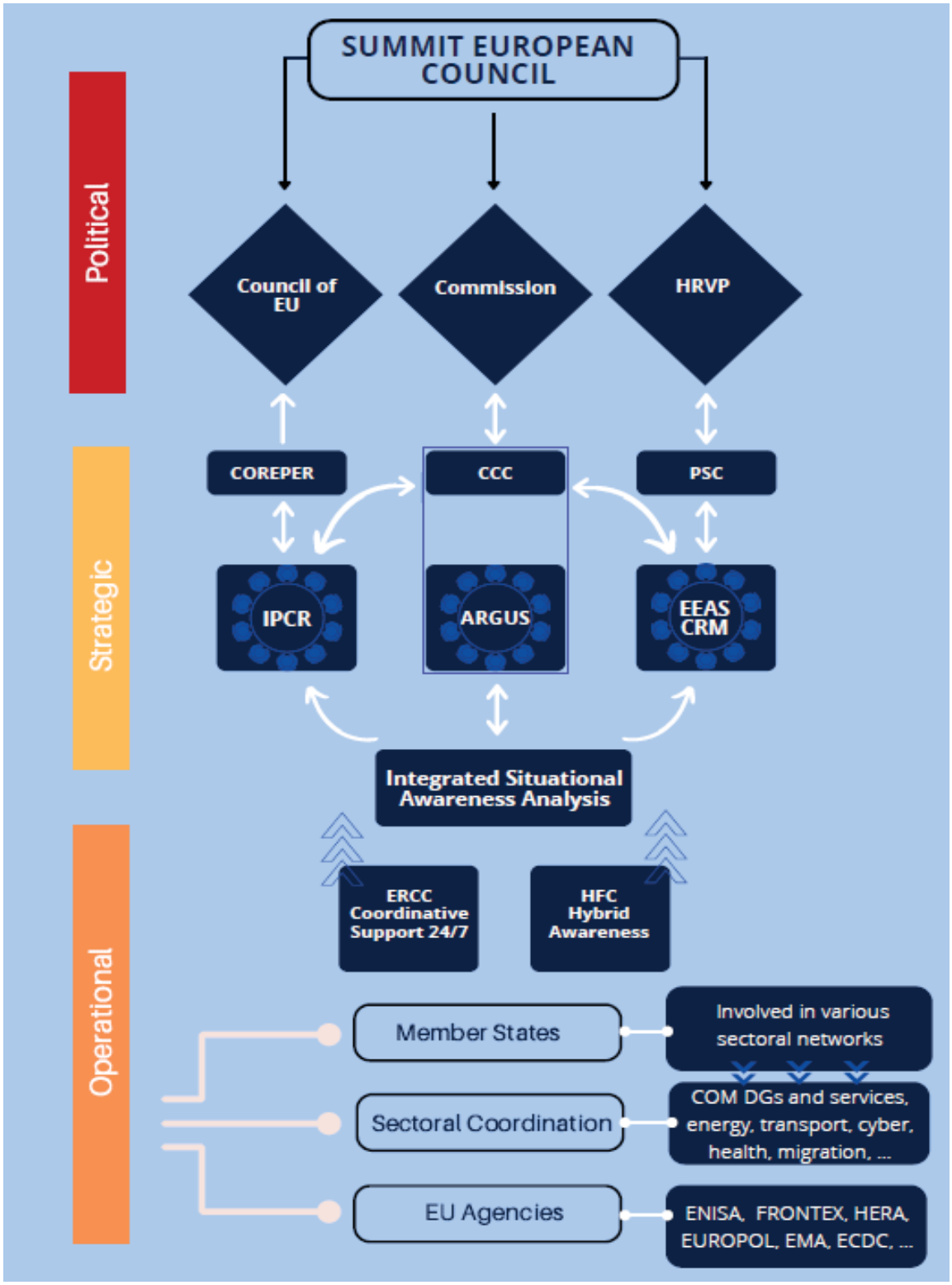
- The **Emergency Response Coordination Centre (ERCC)** of the Commission is the largest and fastest EU operational coordination facility, which supports the EU in any type of crisis, including in a hybrid context. Available 24/7, it coordinates the rapid mobilisation of emergency response capacities in the form of in-kind assistance, modules and teams from Member States and Participating States to the Union Civil Protection Mechanism and rescEU, the EU's strategic reserve of response capacities. The ERCC includes an in-house analytical cell and is connected to the scientific community and a wide array of monitoring and alert systems, which provide data that the ERCC turns into information for strategic anticipation, as well as operational planning and decision-making. This enables joint and cross-sectorial EU emergency operations on the ground. The ERCC also acts as the central contact point for IPCR, including in case of invocation of the Solidarity Clause.

- The **EEAS Crisis Response Centre (CRC)** serves as the permanent crisis response capability in the EEAS. The CRC's objectives are to provide 24/7 situational awareness to enable informed decision-making in the EEAS and EU institutions before, during and after crises, ensure the safety of EU staff in EU Delegations around the world, and facilitate the consular protection of EU citizens facing crises abroad by supporting EU Member States.

Figure 1: Coordination and decision-making levels

Political	European Council European Commission Council of the EU High Representative
Strategic	ARGUS in the Commission COREPER II, PSC, Integrated Political Crisis Response (IPCR) arrangements, and the rotating Presidency of the Council Crisis Response Mechanism in EEAS
Operational/ support	Generic: ERCC, EEAS CRC, INTCEN Sectoral: Capacities, tools, mechanisms and networks, including cyber, FIMI and disinformation, transport, energy, home affairs, civil protection, space, etc (see the *Inventory of the EU's Crisis Management Capabilities*)

Figure 2: Information flows in support of decision-making in crisis



Points of entry

In the case of a major threat or crisis contacts are made at all levels to activate the relevant crisis procedures.

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

- The President of the European Council,
- The rotating Presidency of the Council of EU (Head of State or Government),
- The President of the European Commission or delegated Vice-President/Commissioner
- The High Representative/Vice-President.

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

- For the Council of the EU, the rotating Presidency (Chair of COREPER II),
- For the Commission, the Secretary General,
- For the EEAS, the Secretary General.

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

- For the Commission: the Secretariat-General (ARGUS secretariat), the ERCC (24/7 operational service), and designated lead services (depending on the nature of crisis),
- For the Council: the General Secretariat of the Council (IPCR Secretariat in case of a crisis and Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats Secretariat in case of a detected campaign/threat),
- For the EEAS: HFC, EEAS Crisis Response Centre and the nominated geographic or thematic service,
- For EU agencies: Directors' cabinets, respective parent DG in the Commission.

Example 3: Instrumentalisation of migrant flows by Belarus (2021)

The 2021 hybrid attack by Belarus involving a migration crisis at the external EU border required a quick and coordinated response. The Commission immediately activated its ARGUS coordination arrangements (Phase I) and the Migration Preparedness and Crisis Blueprint. The EU offered immediate support to the affected Member States through the EU agencies (Frontex, EASO, Europol) by deploying experts and officers, as well as equipment (patrol and transport cars). Lithuania activated the Union Civil Protection Mechanism to which 20 countries responded by offering tents, beds, heating systems, electricity generators, and food items. Coordination with Member States as well as situational awareness were undertaken via the Blueprint Network, which also involved the EU agencies and international partners (e.g. IOM, UNHCR). Monitoring and reporting on the migration flows continued into 2022 through

the Migration Blueprint and other networks and the production of the Integrated Situational Awareness and Analysis (ISAA) reports.

In the Council, the Presidency organized an extraordinary meeting of Interior Ministers linked to the IPCR framework and IPCR roundtables at expert level.

The HFC provided analytical reports and verbal briefings to the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats and the Horizontal Working Party on Cyber Issues.

Example 4: Russia's war of aggression against Ukraine (2022)

The EU response to Russia's war of aggression against Ukraine started before the invasion on 24 February 2022. Following multiple cyber-attacks targeting Ukraine's government websites, the ARGUS system was activated in Phase I, allowing Commission services as well as EU agencies to share daily information on cyber and FIMI activities. In parallel, the Blueprint Network was activated to increase preparedness and situational awareness against possible increased migratory flows. In light of the potential risk of natural gas supply cut, Moldova activated the Union Civil Protection Mechanism on 28 January. This was followed by a request for assistance from the Ukrainian government. Amid the growing and persistent threat of a Russian invasion, the Commission President decided on 22 February to activate ARGUS in Phase II, thus triggering multi-sectoral coordination and convening the CCC. Following the full-scale attack on 24 February, the ERCC mobilised emergency assistance from UCPM Member/Participating States, from the rescEU strategic reserve and from the private sector, including on health and chemical, biological, radiological and nuclear (CBRN) hazards, energy, civil protection, agriculture, transport, demining, reconstruction, and protection of cultural heritage. Monitoring and reporting on the migration flows was ensured through the Migration Blueprint network and ISAA reports provide situational awareness on all the different aspects of the crisis. Other sectoral networks were activated in parallel, such as the Network of the transport contact points.

In the Council, an extraordinary meeting of the Justice and Home Affairs Council took place on 27 February, at which ministers decided to activate the IPCR. The IPCR roundtables involving all Member States and EU institutions, as well as international partners, took place twice (later once) a week, focusing mostly on issues related to refugee reception, protection of children, external border management, humanitarian aspects, war crimes investigations, demining, national contingency plans, export of grain, oilseeds and related products from Ukraine (Solidarity Lanes), support to Moldova, as well as strategic communication.

The HFC provided analytical reports and verbal briefings to the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats and the Horizontal Working Party on Cyber Issues.

7. Lessons learnt

Each exercise and real-life crisis must be completed by identifying and implementing lessons learnt. These lessons should in particular feed back into policy development, prevention and preparedness, contribute to identifying gaps and opportunities for the improvement of crisis management arrangements, training, and then testing these improvements in future exercises and real-life events, thus closing the crisis management cycle.

In the past years, the EU faced a succession of crises, including migration and refuges' massive inflows, the COVID-19 pandemic and the Russian aggression against Ukraine. All services involved in their areas of competence to enable an effective and efficient crisis response, should equally look back at what has worked well and what can be improved when confronted with crisis situations in the future through a process of identifying lessons and implementing translating them into improvements along the entire crisis cycle. Likewise, lessons learnt from exercises, such as the EU Integrated Resolve (Parallel and Coordinated Exercises) in 2017-2018 and 2022 contribute to further increasing resilience to and preparedness for tackling complex hybrid crisis.

8. Communication

Strategic communication in the challenging geopolitical and geo-economic context is key to projecting the success of the EU's crisis management internally and globally, where public perception matters as much as the facts. The EU's main focus is to promote – with positive messaging – clear and reliable information in a timely manner in a way that reaches the large audience.

Lessons learnt from the recent crisis shows that effective tools of fast, simple and clear communication are the best remedies to counter hybrid threats (especially foreign information manipulation and interference, dis- and misinformation). Policy response and coordinated crisis communication must be an integral part of countering hybrid threats. The Spokesperson's Service placed under the direct authority of the President, is a central tool dealing with political communication on behalf of the Commission. It also hosts the spokespersons of the High Representative, which allows fully aligning communication to ensure coherence and an effective internal-external nexus. It has all the tools – such as the daily press briefing, press materials, main social media accounts, and press events – that can be used in a coordinated way and deployed immediately in case of a hybrid threat either in a reactive manner or proactively. This communication is done in cooperation with DG COMM, the EEAS Stratcom Divisions/EU Delegations and the Commission Representations in Member States.

The EU is actively working on further enhancing its toolbox to communicate pro-actively in the hybrid context, especially in times of crises. This includes strengthening existing efforts to increase capacity and capability of the EEAS Stratcom divisions, for the EU to communicate strategically and counter FIMI threats on the global scene. These efforts are underpinned by enhancing the capacities of EU Delegations and CSDP Missions and Operations to communicate and respond to FIMI, in close cooperation with international partners. These efforts are complemented by the continued development of the Network against Disinformation to further deploy the EU's communications services to fight dis- and misinformation.

In the Council, the IPCR Crisis Communicators' Network (CCN) which consists of

communication experts from Member States and EU bodies was set-up to contribute to preparedness in particular through the exchange of best practices and lessons identified.[21] The CCN also contributed to addressing the information challenge both in relation to the COVID-19 pandemic, as well as Russia's war against Ukraine.

Example 5: The manipulation of the debate on famine threats caused by Russia's war of aggression

Russia uses information manipulation and interference and disinformation in a strategic and coordinated manner to influence the global debate about the reasons for the deteriorated global food security situation. By directly blaming international sanctions imposed on Russia for the surge in food prices, Russia aims to shift attention from its own actions (blocking of Ukrainian ports, burning crops and silos, imposing its own restrictions on the export of Russian fertilizers) to blaming Ukraine and what it calls 'the collective West" for the consequences of its own war of aggression. Moscow aims to undermine global support for Ukraine, especially in Africa, Asia and the Middle East, as the most affected by such disruption. Such activities are also observed in diplomatic fora where Russiahas been falsely accusing Ukraine of transporting the majority of grain to the EU in order to pay the West for weapons supplied.

In response, the EEAS and Commission services have taken a number of actions to communicate strategically and respond to this information manipulation and interference. These include the work of the Commission's Network against Disinformation, which has been monitoring and analysing false narratives, to form the basis of recommended actions and counter-narratives in its Fighting the Fallacies reports. The EEAS has further stepped up its cooperation with EU Member States and international partners, in particular the G7 Rapid Response Mechanism and NATO, as well as with other stakeholders in light of Russia's aggression against Ukraine. The EU also keeps explaining to EU citizens, as well as globally, the gravity of challenges and implications of war, while explaining the reasons, purpose and impacts of sanctions imposed on Russia.

9. Cooperation with NATO and other international partners

Contacts with partners at all levels are beneficial for the EU's preparedness to counter hybrid threats as they facilitate cooperation, including at the early warning and crisis management stages. These in particular entail the North Atlantic Treaty Organisation (NATO) and other relevant international organisations and like-minded partners, such as the G7, as well as contacts with civil society and the private sector.

Building on the progress achieved in the past years, EU-NATO cooperation has been strengthened in light of the Russian war of aggression against Ukraine[22]. Cooperation takes place at all levels and covers a wide range of topics, such as situational awareness, strategic

[21] Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements of 17 December 2018.
[22] Detailed most recently in the Seventh progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017, 20 June 2022, https://www.consilium.europa.eu/media/57184/eu-nato-progress-report.pdf.

communication, countering foreign information manipulation and interference, cybersecurity, crisis prevention and response, military mobility, counter-terrorism, resilience of critical infrastructure, and strengthening resilience to CBRN risks. In this context, the Parallel and Coordinated Exercise (PACE) is among the key initiatives of EU-NATO cooperation aiming at increasing resilience to and preparedness for tackling complex hybrid attacks.

In line with the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats[23] as well as the Joint Declarations on EU-NATO Cooperation[24], the High Representative together with the Commission will continue deepening EU-NATO cooperation, in accordance with the agreed guiding principles, namely transparency, reciprocity, inclusiveness and the decision-making autonomy of both organizations, as well as the EU's Strategic Compass.

[23] Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of NATO, July 2018, signed in Brussels.

[24] Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of NATO, July 2016, signed in Warsaw. Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of NATO, July 2018, signed in Brussels; Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of NATO, January 2023, signed in Brussels.