Council of the European Union

Brussels, 8 February 2021
(OR. en)

5986/21

LIMITE

COPS 46
CFSP/PESC 110
CSDP/PSDC 39
POLMIL 14
EUMC 23

COVER NOTE

From:	European External Action Service (EEAS)
To:	Delegations
Subject:	Scoping Paper: preparation of the Strategic Compass

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (21.05.2021)

Delegations will find attached document EEAS(2021)129

Encl.: EEAS(2021)129

EUROPEAN EXTERNAL ACTION SERVICE

Security and Defence Policy Directorate

Working document of the European External Action Service

Of 04/02/2021

EEAS Reference	**EEAS(2021) 129**
Distribution marking	***Limited***
To [and/or GSC distribution acronyms]	**Political and Security Committee (PSC)** **Delegations**
Title / Subject	**Scoping Paper: preparation of the Strategic Compass**
[Ref. prev. doc.]	

Scoping Paper: preparation of the Strategic Compass

Scene setter

The threat analysis has been a first, successful step towards developing the Strategic Compass. Member States have provided answers to the key political guiding questions they received ahead of the FAC on 20 November 2020. This scoping paper presents the outline of the Strategic Compass, based on ideas Member States presented in their answers to the key political guiding questions. This scoping paper identifies the main topics for discussion and should thus help frame the strategic dialogue amongst Member States, also in the Council, that will take place in the first half of 2021. By November 2021, building on these discussions and guidance by Member States, a first draft of the Strategic Compass would be prepared and presented by the HR/VP to Ministers for discussion and guidance. The Commission and the EDA will be closely associated as appropriate throughout this process. The Strategic Compass will have links with a number of EU initiatives managed by the Commission. It would seek maximum synergies in that regard, while fully respecting their governance and the Commission's prerogatives in that respect.

Structure of the Compass

The first part/chapter of the Strategic Compass should reflect the threats and challenges the EU faces (based on the threat analysis and taking into account the EU Global Strategy). The answer to these threats and challenges lies in enhancing the EU's ability to act, autonomously whenever necessary and strengthening cooperation with partners wherever possible. At the same time, the notion that the Strategic Compass contributes to develop the common European security and defence culture, informed by the EU's shared values and objectives, should be well reflected. It should also set out more general principles e.g. respect for international law and the United Nations (UN) Charter, including international human rights law and standards, a rules-based order with multilateralism as key principle, the EU's Integrated Approach, civilian-military cooperation, for example in the fields of human rights and gender. Finally, the importance of strategic communication should be highlighted.

In the second part, the Strategic Compass should first describe what the EU needs to do – in light of the threats and challenges – in the areas of crisis management (first basket) and resilience (second basket) to 'strengthen its ability to act autonomously when and where necessary'. As a consequence to that, it should describe what capabilities (third basket) the EU needs and how the EU can enhance its support to and cooperation with partners (fourth basket).

The Strategic Compass needs to be actionable with precise timelines. It should not only state what is important, but it should set clear **goals** on what the EU and its Member States need to do within the next 5 to 10 years in the area of security and defence. It should stimulate further coherence

between security and defence initiatives that have been launched, mainly since the EU Global Strategy (EUGS) of 2016 and provide clearer **guidance** to implement the EU Level of Ambition that derives from the EUGS. It should furthermore take into account the changes in the security context since the EUGS, including emerging threats and new challenges.

That is why the Compass should **define policy orientations, specific goals and objectives**, as called for by the Council conclusions of June 2020. The ongoing work on security and defence initiatives in the framework of the follow-up to the Global Strategy will also feed into this process while the Strategic Compass should provide coherent guidance for these initiatives and other relevant processes, where appropriate.

Taking the abovementioned considerations into account and based on Member States' inputs, we propose the following structure and concrete functional goals/objectives, with subsequent themes for discussion in the Strategic Dialogue-phase:

***Note**:* It is important to acknowledge that several of the topics mentioned below have a horizontal, cross-cutting nature. This implies that flexibility is needed to adjust the structure throughout the Strategic Dialogue-phase if necessary.

<u>General</u>

1) *Assessment of security threats and challenges facing the Union*

   - Reflect threats and challenges the EU is facing and will face in the near future;
   - Stress general principles, for example the need to adhere to and defend international law (UN Charter), the need to implement the EU's Integrated Approach to conflicts and crises, highlight the EU's unique toolbox including the potential to strengthen civ-mil cooperation, and recognising the complementarity between EU internal security policies and external relations/foreign policy;
   - Implications for the EU as a security and defence actor, acting autonomously when necessary, and being a stronger global security provider (including transatlantic link) and defender of effective multilateralism. Need to strengthen solidarity amongst EU Member States.

2) *Enhance prevention and strategic foresight*

   - Have a regularly updated threat analysis;
   - Enhance the EU's situational awareness;
   - Early warning to early action;

- Foresight function regarding longer term trends that drive security and defence needs/priorities (supply chain, technology, resources/raw materials, implications of climate change and environmental degradation, etc.).

Crisis Management

3) Become a more capable and effective crisis responder and security provider

- Develop a strategic view on CSDP operational engagement towards a 'security belt' around Europe; define political interests for interventions;
- Incentives for force generation/deployment of staff/provision of capabilities and capacities (including early force sensing?);
- More robust/flexible mandates of CSDP mission and operations, also taking into account new modalities enabled by the EPF;
- Enhance flexibility and speed of decision making;
- Explore ways to enhance links between European *ad hoc* operations and CSDP;
- Timely and accurate intelligence to support decision making;
- Enhance effectiveness of missions and operations: further develop existing methods of mandate delivery, management, control and evaluation;
- Strengthen support to host State authorities through civilian CSDP missions in tackling security challenges, in line with the Civilian CSDP Compact (and mini-concepts). Requires stronger CSDP-JHA cooperation;
- Enhance synergies and consistency between CSDP missions and operations and EU financial instruments (NDICI)

4) Increase responsiveness and operational readiness

- Enhanced operational readiness and responsiveness:

  (1) Determine parameters for all types of civilian missions and military missions and operations annexed to the EU Level of Ambition, based on likely/necessary scenarios of future CSDP engagement and ambition;

  (2) Further develop the EU's military planning and conduct (C2) - structures/capabilities, taking into account civ-mil synergies;

  (3) Further develop required capacities for civilian and military rapid response (including a link to EU Battlegroups, Core Responsiveness Capacity (CRC), Specialised Teams);

- Further develop the EU's strategic foresight planning capability to conduct civilian and military advanced and cold planning (linked to the scenarios);
- Regular exercises need to take place, at various levels and of various complexity covering civilian and military scenarios (including conducting live exercises?);
- Explore setting up modules of combat forces under the Full Spectrum Force Package which train and exercise together (in the context of PESCO Strategic Review).

Resilience

5) Secure access to the global commons (incl. cyber, high seas and space)

a. Stronger maritime security actor

- The EU needs to build on/develop its naval CSDP operations and the Coordinated Maritime Presence concept (MS presence in strategic areas) to provide a strong platform to further develop (more permanent?) operational engagement (on a global basis?);
- Respond to geopolitical tensions in maritime domain. The EU needs to protect its interests, for instance to ensure freedom of navigation, safe sea lines of communication, offshore infrastructures etc. In this regard, an enhanced implementation of the European Union Maritime Security Strategy (EUMSS) and its Action Plan is needed;
- Explore possible regular naval exercises (to enhance interoperability and familiarise with the EU context);
- Enhance maritime capacity building and improve maritime situational awareness.

b. Strengthen cyber (security and) defence (in line with the EU Cybersecurity Strategy)

- Work towards comprehensive cyber capability (secure networks, sharing information, training/exercises, response options and teams) also through respective PESCO projects, linking to the EU Cyber Diplomacy Toolbox, EU cyber crisis mechanisms, and to CSDP missions/operations, etc.;
- To this end, a review of the Cyber Defence Policy Framework should allow to step-up cyber defence cooperation and coordination, give impetus to cyber defence capability development, and strengthen synergies between cyber security and defence initiatives;
- Increase the ability of the EU and Member States to prevent, discourage, deter and respond to and recover from malicious cyber activities by strengthening its

posture, situational awareness, tools, procedures and partnerships in the context of the EU Cyber Diplomacy Toolbox.

c. Strengthen defence role in Space

- Enhance situational awareness and geo-intelligence support, building EU (including Satcen) and Member States expertise capacities;
- Ensure link with EU Space Programme (Galileo – including Public Regulated Service (PRS), Copernicus, etc.) and with the European space based secure connectivity initiative as well as recognise opportunities for investment (including under Horizon Europe, EDF) and explore other possible synergies between space and defence (incl. capabilities).

6) *Assess strategic vulnerabilities in security and defence, enhance resilience*

- Operationalise (and further clarify where necessary) existing EU instruments, in line with existing EU policy, and highlight how they contribute to preventing and countering hybrid threats;
- Introducing baseline requirements to be developed for Member States (in synergy and complementarity with Commission work and in coherence with NATO);
- Enhance economic security and protect critical infrastructure (in synergy and complementarity with Commission instruments, link with baseline instruments);
- Enhance resilience of CSDP missions and operations against hybrid threats, including cyber-attacks and disinformation;
- Security of communications/information among EU institutions and with Member States.

7) Enhance mutual assistance and solidarity amongst Member States

- Implement lessons identified from the Art. 42.7 TEU scenario based exercises. Link with Art. 222 TFEU;
- Develop a handbook to be triggered upon activation (setting up a taskforce, linking to other EU instruments such as cyber, sanctions or others, linking to Council emergency procedures, to possible partners (i.e. NATO).

8) Improve military assistance to civilian authorities

- Military role in pandemics (COVID-19, etc.), in the context of humanitarian aid, disaster relief, evacuations, logistics/strategic lift, CBRN…(in synergy and complementarity with relevant EU instruments).

In order to reach these goals the EU needs:

Capabilities

9) Develop the necessary civilian and military capabilities/capacities

- Need to define parameters of coherent Full Spectrum Force Package;
- Develop mobile and deployable military forces and civilian capacities. Member States to focus on jointly developing the necessary, interoperable and sustainable enablers for EU missions and operations;
- Identify next step in Military Mobility as work on the implementation of the Action Plan continues on transport infrastructure (co-funding through Connecting Europe Facility 2021-2027) and procedural and regulatory issues.;
- Deepen defence cooperation amongst Member States (through PESCO, CARD, while making best use of the EDF), while ensuring coherence among EU defence initiatives; promoting new financial incentives;
- Need to further develop a comprehensive civilian capacities pool based on the Civilian Capability Development Plan as part of the Compact implementation.

10) Improve capability development processes

- Provide political/strategic guidance for CDP revision(s) and subsequent HLG-cycles;
- Streamline capability planning and development processes (CDP, HLG/HICGs, PESCO, CARD) and continue coherence of output with respective NATO processes, notably the NDPP;
- Embedding EU military capability development processes in national defence planning processes and make best use of EU defence initiatives (through PESCO, CARD);
- Further develop civilian capability development process, in line with Civilian CSDP Compact. What to do beyond 2023?

11) Promote technological sovereignty and innovation

- Increase defence R&T spending through PESCO, CARD, and incentivise investments in R&T through EDF;
- Reflect on the impact of emerging technologies to ensure that new and disruptive technologies could be applied and used across the EU, facilitate research and innovation in emerging technologies, and increase the EU's resilience, for instance by reflecting on the:
    - impact of Artificial Intelligence (AI) in security and defence, including the malicious use of this type of technology (forefront of new technologies, link to normative and legal aspects, link to wider Commission work including on the availability of data for security research and innovation) and the use of AI by Member States against these threats;
    - implications/inclusion of automated systems for future CSDP missions and operations (use of drones, AI applications…).
- Link to climate and defence – circularity, energy and resource efficiency, innovative technological solutions, environmental footprint, set objectives;
- Ensure clear link with defence industry - highlighting the importance of an innovative and competitive EDTIB as well as identify strengths and vulnerabilities of defence industries. (synergies with Commission actions); .
- Guarantee security of supply/supply chains and security of supply (both within EU and from outside), including raw materials, critical components and technologies.

<u>Partnerships</u>

12) Strengthen partnerships in security and defence

a. Structural and enhanced cooperation with international organisations in different domains:

- UN: particularly enhancing cooperation in the framework of the EU-UN partnership in crisis management (including promotion of International Humanitarian Law, Human Rights, WPS and UNCLOS), at various levels, including closer cooperation and coordination;
- NATO: reinforce cooperation in light of common challenges and further strengthening our strategic partnership and cooperation in all areas of interaction;
- OSCE, AU, ASEAN, ECOWAS, G5 Sahel, etc.

b. Develop a more strategic approach towards partnerships with third countries in security and defence

- Overarching Partnership Architecture;
- Bilateral partnerships in security and defence;
- Cooperation in specific thematic sectors (cyber, hybrid, maritime, etc…);
- Capability development (where possible through PESCO);
- Participation in CSDP missions and operations.

c. Enabling and supporting partners in dealing with their security by themselves

- Cooperation with partners for training and capacity building;
- Support resilience to hybrid threats and cyber capacity building in third States;
- Support security sector governance and reform, complementing activities, funded by the EU (such as NDICI) or bilateral means in the area of peace and security;
- Effective implementing the European Peace Facility.

Annex: Roadmap for the strategic dialogue in the first half of 2021

DELETED FROM THIS POINT UNTIL THE END OF THE DOCUMENT (page 13)