Council of the
European Union

Brussels, 13 May 2015
(OR. en)

8887/15

LIMITE

COPS 148
CSDP/PSDC 274
CFSP/PESC 153
POLMIL 59
EUMC 20
CIVCOM 83
COEST 140
COAFR 172
COTER 67

COVER NOTE

From:	European External Action Service (EEAS)
To:	Political and Security Committee (PSC)
Subject:	Food-for-thought paper "Countering Hybrid Threats"

Delegations will find attached document EEAS(2015) 731.

Encl.: EEAS(2015) 731

EUROPEAN EXTERNAL ACTION SERVICE

CMPD – Crisis Management and Planning Directorate

Working document of the European External Action Service

of 13/05/2015

EEAS Reference	**EEAS(2015) 731**
Distribution marking	***Limited***
To [and/or GSC distribution acronyms]	**Political and Security Committee Delegations COPS-CSDP/PSDC-PESC-CIVCOM-COAFR-COEST-COTER**
Title / Subject	**Food-for-thought paper "Countering Hybrid Threats"**
[Ref. prev. doc.]	**-**

Food-for-thought paper
"Countering Hybrid Threats"

1. This document outlines a possible way ahead for the EU to better support MS, and itself, in countering hybrid threats, in accordance with the direction given by Defence Ministers at their meeting in Riga in February 2015. It should be read as a chapeau document and in the context of the decision taken to bolster EU Stratcom in response to recent hybrid threats.

Hybrid threats – the context

2. During the course of the past year, Europe's security environment has changed dramatically, with two key developments dominating security agendas.

3. To the East, Russia's aggression in Ukraine, including the annexation of Crimea, has challenged the core principles of international law. Russia's sophisticated use of large-scale, well-coordinated hybrid warfare tactics has compromised Ukraine's territorial integrity and has strived to destabilise the larger neighbourhood. Further, through ambiguity and veiled threats, they have been seeking to divide the international community, including the EU which they often portray not merely as a biased party but also as the instigator of the conflict.

4. To the South, the advances and morphing of Da'esh, has fuelled regional instability with worrying signs that their appeal is spreading to other insurgent groups, such as Boko Haram and Al Shabaab. Closer to home, Da'esh's expansion and aggressive ideology has tempted thousands of young Europeans away from traditional European values into joining the jihad as "foreign fighters". There are significant consequences for Europe when these fighters return home.

5. Recently issued non-papers by Member States have urged the EU to examine possible responses that could enable MS to build resilience to hybrid threats and, within that context, to improve the quality and method of European strategic communication.

Defining hybrid threats

6. Hybrid warfare can be more easily characterised than defined as a centrally designed and controlled use of various covert and overt tactics, enacted by military and/or non-military means, ranging from intelligence and cyber operations through economic pressure to the use of conventional forces. By employing hybrid tactics, the attacker seeks to undermine and destabilise an opponent by applying both coercive and subversive methods. The latter can include various forms of sabotage, disruption of communications and other services including energy supplies. The aggressor may work through or by empowering proxy insurgent groups, or disguising state-to-state aggression behind the mantle of a "humanitarian intervention". Massive disinformation campaigns designed to control the narrative are an important element of a hybrid campaign. All this is done with the objective of achieving political influence, even dominance over a country in support of an overall strategy.

7. A critically important aspect of hybrid warfare is to generate ambiguity both in the affected population under attack and in the larger international community. The aim is to mask what is actually happening on the ground in order to obscure the differentiation between war and peace. This ambiguity, the lack of full attribution, can paralyse the ability of an opponent to react effectively and mobilise defences as it becomes unclear who is behind an attack. Even more, ambiguity can divide the international community, limiting the speed and scope of a response to the aggression.

By design, hybrid threats will continuously evolve based on the success of their application, continuing technological developments, changes in potential adversaries' vulnerabilities and developments in measures to counter them. The important factor for the EU is to be able to recognise the overall effect and build resilience as a means of countering the attack.

Recognising vulnerabilities

8. The fundamental characteristic of hybrid attack is that it is designed to exploit a country's vulnerabilities. It is essential that MS and partners recognise this fact and draw the appropriate political and operational conclusions in order to respond.

9. In Ukraine's case, the country's critical vulnerabilities were related primarily to (i) weak governance and national institutions, wide-spread corruption; (ii) lack of trust and support for security and defence structures; (iii) the presence of a large Russian speaking population that perceived itself marginalised; and (iv) critical dependency on Russia for imports and energy supply.

10. For MS the threat from Da'esh exposes very sensitive issues. The vulnerabilities associated with the integration of minorities and social exclusion on the one hand, and an inherent weakness that stems from an open society (underpinned by free speech) on the other, have made it difficult to react to the spread of hatred. Furthermore in defence terms, our political system has been traditionally focussed on a response against state actors, and today we collectively ill-prepared to resist the hybrid threats that emanate from non-state actors and those engaged in war by proxy.

11. As such, all MS have vulnerabilities. They largely vary and range from economic and energy dependencies, heavy reliance on critical infrastructure in key areas, such as finances, energy, communications or transport, to the very subtle and sensitive issues within countries surrounding integration of religious or ethnic groups or deficiencies in respecting human rights.

12. Looking inwards, the EU as an institution needs to assess its own vulnerabilities too, at Headquarters and abroad alike. This includes the vulnerabilities of its CSDP Missions and Operations that are deployed in high-risk areas, where they can become targets of subversive threats.

13. While national vulnerabilities are fundamentally country-specific, a number of them represent challenges for many if not all MS. Cyber vulnerabilities for instance are a cause for concern

for all – even if the level of preparation and capacity to counter malicious activities varies considerably from country to country. The fact that we are increasingly interconnected is also a strong argument in favour of complementing national efforts with collective ones.

14. Given the high degree of dependence on energy supplies from abroad, many MS are vulnerable if their supplies are not sufficiently diversified. The EU already offers an exemplar with its template for resilient energy union and it is critical that the experience gained in this field is applied more widely.

15. The first step on the road to enhancing our capacity to withstand hybrid attacks is to recognise our vulnerabilities. Only then will we be able to reduce the "surface of the attack" and devise proper steps nationally and collectively. Recognising such weaknesses often proves difficult even nationally – and a lot more so in larger communities, like the EU. These are matters of national sovereignty and many of the issues involved are extremely sensitive.

EU Response

16. There are four key questions that the EU should consider: What can we do to counter hybrid threats? How can we address the root causes? How can we reduce vulnerabilities? Can we use the tools we already have in a more coherent way?

Improve awareness

17. Foremost, it is vital we understand our vulnerabilities, and to do this we need to acquire and maintain a sufficient level of situational awareness. It is important to be able to recognise any subtle changes to the threat landscape, which later may turn out to be elements of an adversary's larger campaign. Effective awareness is a fundamental requirement and must be supported by better information and intelligence sharing and also the sharing of existing best practices and lessons learnt. Within the European institutions there needs to be much closer contact between relevant bodies that are exposed to or have sight of hybrid threats and indicators; at the moment, we lack that focal point.

18. Having canvassed broadly within the Service and the Commission, there is a general view that we already have access to a good number of the indicators and warnings from across the broad range of EU competencies that could support a very effective form of early warning. A virtual "market place" located in the EEAS where MS and the Institutions could share relevant information, and draw on the full gamut of EU competencies, could bring clarity by analysing the various indicators and alarms triggered by hybrid action. This virtual fusion cell could include elements such as strategic foresight and early warning and be supported by scientific research. With appropriate joint tasking, it would be relative straight forward to bring the appropriate competencies together to give a focus to our analysis and importantly identify the best EU instruments for response.

19. In detail, the cell could catalyse all indicators from the EEAS services, including EU Delegations and the COMMISSION services, and other key partners – both countries and organisations, such as NATO, and then analyse them against a possible hybrid attack scenario both in EU MS and third countries. The EEAS provides the natural focus for this intelligence

led work. This action would represent a quick win and has no significant resource implications as it could be the function of prioritised tasking.

Building Resilience

20. First and foremost, it must be accepted that responding to and countering hybrid threats is and will remain a national responsibility and for good reason. It is the responsibility of the given country to reduce its critical vulnerabilities. Nonetheless the EU could, subject to agreement among MS, provide a platform that can help boost the effectiveness of national efforts aimed at countering hybrid threats by for instance establishing common benchmarks to harden the protection of national infrastructure or build appropriate storage to reduce sudden shortages in energy supplies.

21. The goal in early phases of a hybrid attack is often to create an internal security challenge; and as such, internal challenges require MS to respond through the use of its own instruments. Complex attacks will often aim to swamp a government and lead to the end phase of a hybrid attack being underpinned by the application or the threat of application of a conventional force. This is where smaller countries can draw support from membership of international organisations and alliances.

22. Resilience can be defined as having the capacity to withstand stress and catastrophe. Stress in a society is best bounded by a strong political system that is underpinned by good governance and freedoms that take full account of human rights. Work to bolster the effective application of the rule of law, fight corruption or reform the funding of political parties are key ingredients in the defence against hybrid attack. In the area of critical infrastructure protection increasing the minimum security requirements can help significantly reduce dangerous vulnerabilities.

23. The EU, by drawing on its wide array of instruments and expertise, could also play a central role in supporting its neighbours and partners to become more resilient to hybrid threats. This includes the use of our versatile CFSP/CSDP tools for promoting capacity-building, conducting training and exercises with partners.

24. There is also a unique opportunity begging. Neither the EU nor NATO currently has a strategy to counter hybrid threats. Given the fact that both organisations bring different competencies to bear, there is the rare chance to collaborate on building complementary and mutually supportive strategies while retaining the autonomy of actions in both organisations. This work would go a long way to answering the call made in Wales and by recent MS non-papers.

Deterring Aggression

25. It is imperative to demonstrate convincingly to the potential adversary that the attack will have consequences and aggressors must pay a price. Deterrence works in two ways: through punishment, i.e. a certain course of action may lead to counter-measures that will hurt or through the denial of the benefit of the attack, for instance by considerably enhancing the protection of critical infrastructure or that of the society. CSDP again offers an extra dimension to the EU quiver in supporting partners.

26. Seeking new ways of cooperation with NATO could significantly enhance both organisations' toolbox in deterring and responding to hybrid threats.

Responding to attack

27. A prime feature of hybrid attack is to create uncertainty about what has been happening and who stood behind the attack. Confusion over attribution weakens the resolve of countries, and in particular that of consensus-based organisations, to take decisions on the response to an attack. This, in turn, risks weakening the potential inherent in membership of organisations, like the EU or NATO. It is, therefore, imperative for MS to accept that in hybrid warfare full attribution and undeniable proofs that can stand before the court is not always possible – a premise that they should be able to adapt to when taking decisions.

28. For the EU swift decision-making at the political level remains critical to successfully prevent and defend against future hybrid threats. Hybrid threats also demand a fundamentally different mind-set where traditional separation lines between internal and external, defence and homeland security, civil and military affairs are no longer easily applied.

29. Information warfare is now an everyday part of the modern environment and consensus-based organisations in particular need to be alert to the fact that it is a contested space. By denying or distorting facts, populations can be easily manipulated, politicians dissuaded. The ability to respond to such attack by employing a sound communication strategy is essential both for the MS and institutions alike. Propaganda can be challenged by fact, but to be effective strategic communication must be well-thought through and reflect the different needs and sensitivities of internal and external audiences. Also we should not forget that propaganda may target not only external audiences but domestic ones too. Large populations can be 'brain-washed' through the manipulation of the media (as we see it for instance in Russia) or by spreading false hopes and hatred - a method practised by Da'esh and other terrorist groups.

EU role in countering hybrid threat – an institutional perspective

30. In responding to hybrid threats we need to recognise where our competencies lie and what are the areas more specifically where MS would see merit in receiving help for the EU.

Recommended Actions

31. As we prepare for the June European Council on Defence there are three key actions that could kick start further work on EU's response to hybrid threats:

(1) Ensure that the need to counter hybrid threats is linked to the upcoming Strategic Review and action noted in the June EC conclusions

- It is important to demonstrate that there is solidarity at the level of HoSG that countering hybrid threats is important to the EU's defence and security.

(2) Develop an EU-wide strategy to counter hybrid threats – and do it in a way that is complementary to NATO's similar efforts

- Given the complexity of hybrid threats a strategy is deemed essential to provide the policy framework and guidance for a coherent EU action;

- Neither EU nor NATO currently have a strategy to counter hybrid threats – therefore there is a unique opportunity for them to work in a mutually supportive manner;

- Examine the possible contribution of and implications for CSDP in terms of intelligence sharing, training/exercises and capacity-building with partners.

(3) Improve EU's situational awareness

- Establish, **as a matter of priority**, a virtual EU hybrid fusion cell that could act as a focal point for indicators and warnings of hybrid attack that are noted by the EU institutions;

- Use this cell as a point of entry for all MS and partners who have experienced hybrid attack and who wish to share intelligence or lessons identified.

(4) Step up EU Strategic Communication

- Improve the EU's ability to communicate its messages towards Russia and the Eastern Neighbourhood, and to respond to disinformation when it appears;

- Prepare by June an action plan on strategic communication, as per the tasking of the June European Council.