Council of the European Union

Brussels, 5 May 2021
(OR. en)

8448/21

LIMITE

EUMC 100
CSDP/PSDC 232

COVER NOTE

From:	European External Action Service (EEAS)
To:	European Union Military Committee (EUMC)
Subject:	EU Guidance on countering Hybrid threats during the planning phase of EU-led CSDP military operations and missions

Delegations will find attached the EU Guidance on countering Hybrid threats during the planning phase of EU-led CSDP military operations and missions, as agreed by EUMC under silence procedure on 4 May 2021.

Encl.: EEAS(2021)90 REV 3

EEAS (2021)90 REV 3
LIMITE
EUROPEAN EXTERNAL ACTION SERVICE

European Union Military Staff

Working document of the European External Action Service

of 04/05/2021

EEAS Reference	**EEAS(2021)90 REV 3**
Distribution marking	**LIMITE**
From **To**	**European Union Military Committee (EUMC)** **European Union Military Committee (EUMC)** **CSDP/PSDC; EUMC**
Title / Subject	**EU Guidance on countering Hybrid threats during the planning phase of EU-led CSDP military operations and missions**
[Ref. prev. doc.]	**EEAS(2021)90 Rev2**

Delegations will find attached the EU Guidance on countering Hybrid threats during the planning phase of EU-led CSDP military operations and missions, as agreed by EUMC under silence procedure on 04 May 2021.

TABLE OF CONTENTS

REFERENCES

A. Joint Framework on Countering Hybrid Threats – a European Union response, JOIN (2016) 18 final, dated 6 Apr 2016.

B. EU Concept for EU-led Military Operations and Missions, doc 14777/19, dated 03 Dec 2019.

C. EUMC Glossary of acronyms and definitions - Revision 2020

D. Multinational Capability Development Campaign (MCDC) project: Understanding Hybrid Warfare (January 2017).

E. Multinational Capability Development Campaign (MCDC) projects: Countering Hybrid Warfare (March 2019).

F. Multinational Capability Development Campaign (MCDC) project: Countering Hybrid Warfare - guidance for military planners (2021).

G. The Landscape of Hybrid Threats: A Conceptual Model – EU JRC CoE CHT, WK 13852/2020, dated 30 Nov 2020.

1. Introduction

1.1. The 2016 Joint Framework on Countering Hybrid Threats – a European Union response (Ref. A) foresees 22 actions ranging from improving information fusion and situational awareness, to protecting critical infrastructure, cybersecurity, building resilient societies. Some of the actions aim to enhance EU-NATO cooperation on countering hybrid threats.

1.2. Action 21 of the Joint Framework reads "The High Representative, in coordination with Member States, will integrate, exploit and coordinate the capabilities of military action in countering hybrid threats within the Common Security and Defence Policy" and directly addresses the military contribution to countering Hybrid threats within Common Security and Defence Policy (CSDP).

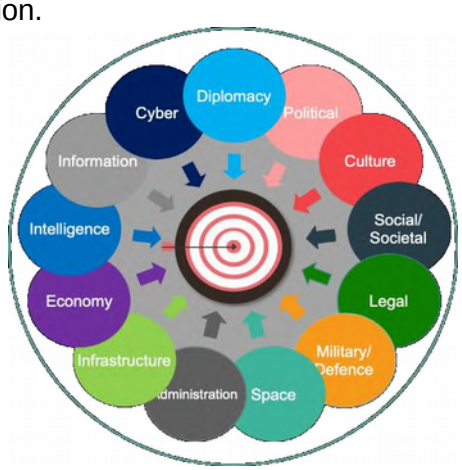
1.3. The updated version of the concept for EU-led military operations and missions was approved in December 2019 (Ref. B). The concept reflects the latest conceptual developments in planning and conducting military operations and missions including countering hybrid threats.

1.4. To describe countering hybrid threats aspects in more detail for EU-led CSDP military operations and missions the decision was taken to develop a Guidance on countering hybrid threats.

1.5. This document was developed from discussions with and documents from the Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare Projects, primarily the MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare (January 2017, Ref. D), Countering Hybrid Warfare (March 2019, Ref. E) and Advice and guidance to military planners (2021, Ref. F) [1].

1.6. Hybrid tactics are in fact not new, they are as old as war itself. However, the term "hybrid" has recently been used to capture the increased complexity of war, t multiplicity of actors involved and the blurring between traditional categories of conflict.

1.7. Figure 1 below demonstrates that hybrid threats activities targets a state(s) in multiple domains. The attacker seeks to undermine and destabilise its opponent through applying both, coercive and subversive tactics, including various forms of sabotage, disrupting communications, energy supplies and could work through empowered proxy groups. All this done with the objective of achieving influence and dominance over the country or region.



[1] https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare

Figure 1. Hybrid threats complexity[2]

1.8. In general, Armed Forces will most likely not be the leading organization within a hybrid crisis response. However, Armed Forces are fit to support decision-making of other governmental organizations and function in a multinational, interagency approach.

1.9. Hybrid threats are designed to exploit vulnerabilities across the political, military, economic, social, informational and infrastructure (PMESII) spectrum by using military, political, economic, civilian and informational (MPECI) instruments of power. Therefore, as a minimum the commander of a military operation or mission should conduct a self-assessment of critical functions and vulnerabilities across all sectors, and maintain it regularly. Additionally, commander should be aware also of these out-of-area yet mission-related vulnerabilities, and ensure that other actors are tasked to gap them or to mitigate the related risks.

1.10. Crucially, the analysis of different actions must consider how these means of attack could be formed into a synchronized attack package tailored to the specific vulnerabilities of its target. Hence, a comprehensive military and civilian approach along with continuous cooperation with all relevant actors in an inclusive way for all EU MS, is significant for a safe and secure environment in Area of Operation (AOO)/Mission Area (MA).

2. Aim and scope

2.1. The aim of this document is to introduce a guidance on countering hybrid threats and their impact during the planning phase of CSDP military operations or missions.

2.2. It is primarily aimed at military personnel working at the military strategic, operational and tactical levels. However, it is also recommended for civilian personnel to understand the military contribution to countering hybrid threats on the CSDP military operations and missions.

2.3. The guidelines mentioned in the document are primarily intended for planning phase of CSDP military operations and missions; nevertheless, they can also be applied during the planning of civilian missions and beyond the CSDP framework.

2.4. Given the evolving nature of hybrid threats, these Guidelines are considered as a "living document" which requires constant development based on feedback from practitioners.

3. Characteristics and actors of Hybrid threats

3.1. Characteristics. The following are characteristics of hybrid threats:

3.1.1. Hybrid threats consist of a wider set of military, political, economic and civil, and information (MPECI) tools and techniques that cannot usually be found at traditional threat assessments.

3.1.2. Hybrid threats target vulnerabilities across societies in ways that we do not traditionally consider.

3.1.3. Hybrid threats synchronize their means in novel ways. By only looking separately at the different instruments of power an adversary possesses, one cannot necessarily predict how and to what degree they might be synchronized to create certain effects. Thus, the functional capabilities of an adversary, although important, will not necessarily provide the right information to understand the problem.

[2] The Landscape of Hybrid Threats: A Conceptual Model – EU JRC CoE CHT, WK 13852/2020, dated 30 November 2020. .

3.1.4. The very complex nature of cyberspace and the information domain make them the preferred attack vectors to launch a hybrid campaign. Indeed hybrid threats intentionally exploits ambiguity, creativity, and our understanding of war to make attacks less "visible", in particular by attacking in and throu cyberspace. This is because they can be tailored to stay below certain detection and response thresholds, including international legal thresholds, thus hampering the decision process and making it harder to react to a Hybrid attack.

3.1.5. Hybrid threats, more than conventional types of warfare campaigns, may not be identified as such until it is already well underway, with damaging effects having already begun manifesting themselves and degrading a target's capability to defend itself.

3.2. Actors

3.2.1. The liberal international order is clearly changing and increasingly under pressure and hybrid threats are very much connected to this. Globalisation, migration, the new geopolitical complexity, the changing nature and balance of power, dazing digitalization's acceleration and increasing ease of access of individuals to technological and social resources, have raised vulnerabilities within states and societies to unprecedented high levels and are changing the security paradigm. This has resulted in a complex and ambiguous situation with severe challenges for International Institutions and States. Hybrid actors use the current transformation processes together with the emergence of new technologies by exploiting vulnerabilities of institutions, states and societies in order to change the international order in their own favour.

3.2.2. Hybrid actors include states, organizations, individuals and have developed well-established techniques to conduct malicious activities. These actors often employ low-cost, low-risk, and high-reward tactics. They are first movers and use marginal technological advantages, meaning that their activities can be fully under way before they are noticed. They are less restricted by legal and ethical constraints, therefore the broad range of techniques make it difficult to identify and counteract their campaigns.

3.2.3. By using different media channels, the hybrid actors may seek to discredit EU legitimacy and credibility. Therefore, appropriate implementation of STRATCOM by defining communication objectives, themes and target audiences is essential to effectively counter disinformation and strengthen the EU's credibility within AOO/MA. Additionally, STRATCOM activities should be coordinated among the EU military and civilian institutions and on a case-by-case basis, with NATO, when a common approach is conceivable.

3.2.4. Hybrid actors pursue their interests by taking advantage of ambiguity and gradual shifts in rights and norms, perverting the principle of "rule of law" to one of "rule by law". That means also that hybrid threats mask the true objectives of an adversary, which severely hinders the ability of a victim's Decision-Action cycle to respond. Hybrid actors influence where they have an asymmetric advantage – mostly in non-military domains – and can exploit vulnerabilities, across the whole spectrum.

3.2.5. There are many types of state and non- state actors in today's complex world environment. Typically, our possible adversaries might be creating hybrid threats by leveraging at least two of the following key entities:

- Military force,
- Nation-state paramilitary force (internal security forces),

- Insurgent groups,
- Guerrilla units (irregular forces operating in territory),
- Mercenaries,
- Foreign intelligence services,
- Transnational or subnational political movements,
- Criminal organizations (gangs, drug cartels or hackers),
- Transnational corporations,
- News media,
- Idealists,
- Hacktivists,
- Amateur hobbyists,
- Religious movements,
- Foreign fighters.

3.2.6. Hybrid actors may cooperate by pursuing common objectives, thus allowing them being adaptive and difficult to define. Actors might apply hybrid threats to achieve their goals by combining regular, irregular and criminal tactics. Adversaries may operate from territories of several states by using secret operations to hamper EU's forces activities in an AOO/MA. The operation/mission related actions from or against an EU Nation(s) cannot be excluded too. Hybrid actors could seek to undermine the legitimacy and trust in the EU's forces in the eyes of the local population, thus could seriously hamper mission objectives, effectiveness and have political consequences. Additionally, terror and fight between criminal groups might also create a serious negative impact on both the security and economic domains.

3.2.7. By using hybrid means, adversaries might influence the EU's forces to employ different counter actions in their favour and allowing shifting actions and achieving the desired effect. However, to challenge the EU military presence in an AOO/MA, adversaries must have both the capabilities and the intention to do so.

4. Countering Hybrid threats

4.1. Setting strategic goals

4.1.1. The **first step** on countering hybrid threats is to identify the threat. Once the threat has been recognized, the next step is to decide what to do about it. The level of ambition for countering hybrid threats will not be the same for every actor. It will depend on context, threat intensity, political appetite and capacity for counteraction. Available policy choices may range from simply absorbing attacks, to deterring aggression, to taking more assertive or retaliatory measures to disrupt on going and prevent further attacks.

4.1.2. These policy choices are articulated through setting strategic goals. These goals should be established prior of counter hybrid threats and revisited continuously in a dynamic strategic environment. All measures and actions taken to counter hybrid threats must contribute to achieving one or more goals. There are three generic strategic goals for any actor designing a strategy to counter hybrid threats.

- Strategic Goal 1: maintain capacity for independent action. The most basic goal is to maintain governmental capacity and capability for independent action. As well as combatting the effects of hybrid threats on the basic functioning of government and society, this goal is also a pre-condition for any subsequent goals. Government and society must build

resilience against hybrid threats by evaluating vulnerabilities and establishing a common and coordinated approach to addressing them through a wide range of tools.

- Strategic Goal 2: deter an adversary from hybrid aggression. A second, more demanding goal is to deter an adversary from conducting hybrid threats. While actions to maintain the capacity for independent action may have deterrent effect (through deterrence-by-denial), comprehensive deterrence requires going beyond resilience to threaten or impose costs (deterrence-by-punishment or sanctions in case of state hybrid actors). Hybrid deterrence should be established from the onset and re-established if it fails, with thresholds set taking into account the defenders' interests and the adversary's intent and capability.

- Strategic Goal 3: disrupt or prevent an adversary from taking further hybrid aggression. The third and most demanding goal is to prevent an adversary from further hybrid aggression. This goal moves beyond deterrence towards measures that will disrupt and degrade an adversary's capacity for action, with regards to national and international laws (although these measures possess deterrent value in their own right). This goal is required because a hybrid adversary may be unlikely to change their behaviour without retaliation designed to degrade their ability or will to carry out hybrid aggression.

4.1.3. There are a number of principles to consider when setting strategic goals. These are detailed below.

- Level of goal-setting. Goals should be set at the governmental and multinational level, for the problem of hybrid threats may only be solved in the strategic and political level through a comprehensive approach.

- Reinforcing the rules-based international order. Setting goals and taking actions to counter hybrid threats should reinforce the rules-based international order and strengthen the seams in liberal- democratic societies exploited by hybrid actors. To retain capacity for action, tactical or short-term activity that might harm or undermine the rules and norms that stabilize the strategic environment should be avoided.

- The consequences of success. If effective formula for countering hybrid threats were to be found, hostile actors that remain motivated may seek alternative or more dangerous ways to demonstrate their grievance. Even setting the threshold for responding to hybrid attacks too low may create a tense and hostile strategic environment in which miscalculation, misperception and escalation become more likely.

- Surprise is inevitable. In setting goals EU Military operations and missions commanders must be ready for shocks, surprises, adaptation and innovation by competitors and adversaries who will always seek to be one step ahead. Hybrid attacks rarely follow a template, so goals and strategies must be reviewed and amended accordingly.

4.2. Setting thresholds

4.2.1. The **second step** is to set thresholds to guide decision-makers in considering when to take specific action to counter hybrid threats. Thresholds are central to setting strategic goals for two main reasons.

4.2.2. First, as it is not possible to respond to every incident of hybrid threat, thresholds must be set according to what level of hostility can be reasonably

tolerated and what level requires countering. While thresholds can be tailored across the PMESII domains, the synergistic nature of countering hybrid threats requires constant monitoring across all entire environments as a whole, rather than by domain.

4.2.3. Second, hybrid adversary's purposefully target their opponent by operating below known or perceived response thresholds to avoid decisive retaliation. Therefore, great care should be taken over communicating response thresholds to hybrid aggression or provocation – including how or whether they are communicated and the consequences of not sticking to them.

4.3. Countering hybrid threats framework

4.3.1. If the strategic goals are the 'ENDS' of an overall strategy to counter hybrid threats, then the 'WAYS' and 'MEANS' required to achieve them are represented by the following three components of the countering hybrid threats framework.

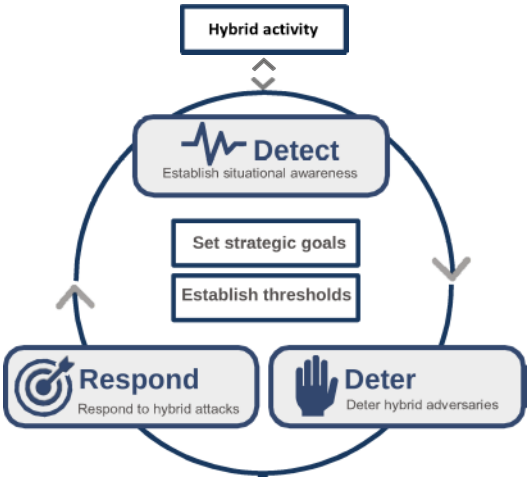


Figure 2. – Countering hybrid threats framework

4.3.2. Detect. This component addresses the problem of detecting hybrid threats or attacks in the first place. Two separate categories "known unknowns" and "unknown unknowns" should be taken into consideration as warning factors for intelligence to detect potential future hybrid attacks. The EU Hybrid Fusion Cell at INTCEN could be one of the capability for the detection and monitoring of the hybrid threats.

- Known unknowns refer to modes of hybrid attacks that we know we may be unaware of it. However, risk related to hybrid attacks may also exist where we are not even aware of its nature, our vulnerability to it, or even of our own ignorance to the threat, this is the field of unknown unknowns.
- Importantly, the practice of discovering unknown unknowns need not sit in opposition to practices of monitoring in itself, but does require a different type of monitoring focused on detecting anomalies and developing practical techniques to recognize previously unseen patterns.

- A useful way of developing this concept for countering hybrid threats by warning intelligence is to differentiate monitoring from discovery:
  - **Monitoring** involves a process of scanning the environment for known unknowns – usually with the aid of indicators – to look for a set of preconceived information about possible hybrid attacks.
  - **Discovery** involves an attempt to manage the problem of unknown unknowns. This process involves capturing and then correctly interpreting information related to a potentially hostile adversarial action that has not been previously conceived. This type of information is not amenable to a monitoring methodology built upon "perceiving what we expect to perceive" via either pattern recognition or the use of indicator lists. This is because the analyst has never seen this pattern before, and cannot be equipped with an indicator list for a type of attack that has never occurred or even been imagined before.
- Figure 3 below shows the basic idea of distinguishing between "monitoring" and "discovery" in warning intelligence for hybrid threats.

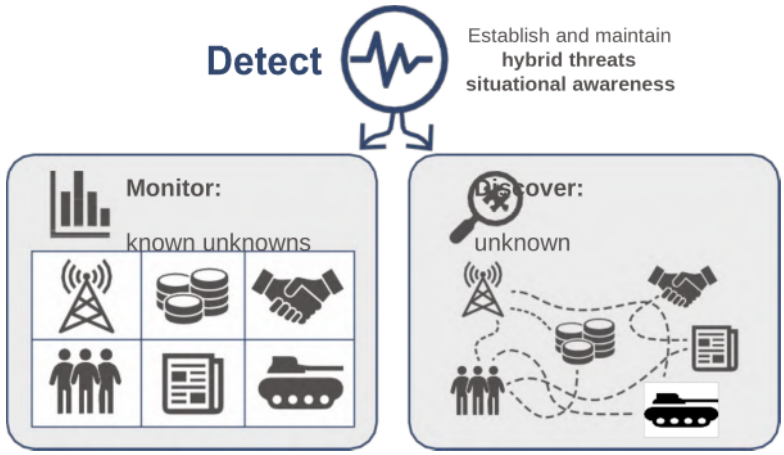


Figure 3. – Distinguishing between "monitoring" and "discovery" in warning intelligence fo hybrid threats

4.3.3. Deter. Deterrence is perhaps the most important tool for countering hybrid threats, simply because it can prevent attacks occurring in the first place. However, the characteristics of hybrid threats serve to complicate the traditional deterrence. Effective "hybrid deterrence" therefore requires updating traditional approaches to deter modern hybrid threats. There are five key principles of effective deterrence on countering hybrid threats:

- Traditional deterrence remains vital. The rise of hybrid threats can be traced to both successes and failures of traditional deterrence. Where traditional deterrence has often succeeded in dissuading revisionist actors from resorting to conventional armed aggression, it has often failed to dissuade the same actors from conducting hostile activity – in the form of hybrid threats. Traditional deterrence policies should therefore be maintained – and even strengthened – to continue to deter motivated revisionist actors from resorting to armed aggression. Traditional

deterrence also contributes to deterring hybrid attacks, making a hybrid adversary think twice where the threshold for response to such aggression is uncertain.

- Hybrid adversaries are deterrable. Traditional deterrence measures should be complemented by specific measures to deter hybrid adversaries. While the characteristics of hybrid threats may complicate deterrence, the difficulties should not be overstated for four main reasons.
  - Hybrid attacks involve the pursuit of interests by actors within a specific context. This allows adversary intent and capability to be discerned to some degree.
  - Although hybrid threats exploits ambiguity, the specific means used by adversaries are often attributable. Complicated by the very nature of cyberspace, the attribution of some cyber incidents represents a huge technical challenge; nevertheless, it could represent an even harder political one.
  - Hybrid adversaries are vulnerable too. Their weaknesses can be exploited through more assertive responses that creatively combine vertical and horizontal escalation. Hybrid aggression may also be a sign of weakness in itself – towards conventional military, political and normative power.
- The Credibility, Capability and Communication of deterrence look different through a hybrid lens. Effective deterrence of hybrid adversaries rests on the Credibility, Capability and Communication, however these should be interpreted differently in the context of countering hybrid threats.
  - Credibility. Protect and create credible deterrence options by pursuing the following actions:
    a) Develop numerous creative, low-level horizontal retaliation options across the MPECI levers of power that are politically achievable but demonstrate clear resolve.
    b) Bolster the enablers of deterrence action, such as public threat awareness.
    c) Prepare for collective deterrence and multinational action under the EU framework through EU institutional arrangements in anticipation of hybrid attack.
    d) Set clear thresholds for response and stick to them– ensure consistency of rhetoric and actions, but also consider taking opportunities to be unpredictable towards the adversary.
  - Capability. Develop the tools, techniques and procedures to detect a wider range of potential hybrid threats, with more confidence, earlier. Enhance and expand the range of tools available to both address vulnerabilities and prosecute deterrence measures targeted towards the adversary, by exploiting both vertical and horizontal escalation. Develop the coordination mechanisms and culture required to take a comprehensive, whole-of-government and multinational approach to hybrid deterrence policy.
  - Communication. Establish clear and realistic thresholds for deterrence and response. Set too low these will be untenable and potentially counter-productive (not all hybrid threats can be deterred at

all times); set too high they may encourage aggression. Consider the effects of communicating thresholds clearly against maintaining constructive ambiguity. Well-signposted thresholds can avoid miscalculation but the knowledge of "red lines" can encourage aggression just below them. Hidden or vague thresholds may deter through unpredictability, but can also invite miscalculation. Bear in mind that all actions communicate something to someone. The key to successful strategic communications is to understand the audience (Internal – external), understand and exploit the information environment, and integrate words and actions across government. The Centre of Gravity is people's perception.

- Resilience is important – but not enough to change behaviours.
  - It is unlikely that resilience measures on their own will change the behaviour of hybrid adversaries, therefore, if the strategic goals of the defending actor include deterring further hybrid attacks, an appropriate balance must be struck between deterrence by denial and punishment measures.
  - Deterrence by denial measures achieves Strategic Goal 1 and Strategic Goal 2 through enhancing the resilience of government and society, minimizing the consequences of hybrid attacks by securing PMESII vulnerabilities. These measures are activated according to the thresholds for action, and are aimed at addressing the defender's vulnerabilities.
  - A revitalized deterrence by punishment strategy towards hybrid adversaries relies on identifying and communicating credible punitive actions across a wider-spectrum of non-military means tailored towards key PMESII vulnerabilities of the adversary. Deterrence by punishment measures are targeted at the adversary's vulnerabilities, and threatened as punishment should a given threshold of hostility be crossed.
- Pursue a tailored approach to deterrence. Hybrid deterrence is ultimately about marginal gains through tailored deterrence. There are four ways to tailor an approach to deterring hybrid adversaries.
  - Disaggregate the strategy of any "hybrid" adversary. This enables the construction of a tailored deterrence strategy that targets specific elements of the overall campaign. In other words, rather than aim to deter hybrid aggression as a whole, consider a disaggregated version of hybrid threats as a collection of complementary strategies.
  - Seek marginal gains. Just as the power of hybrid threats stems from the cumulative effect of coordinated actions, any approach to deterring them must consider how to tip the balance through small steps. Rather than focus on total or comprehensive deterrence, against complex, gradualist hybrid threats, the most viable approach is through marginal gains and focused targeting of key vulnerabilities (of both the defending actor and the hybrid adversary).
  - Target specific assets that are key to enabling a hybrid campaign. For example, hybrid actors value the use of informational means to sow doubt and confusion, but these can be targeted or threatened in specific ways (through attribution, obstruction and counter-narratives).

- Increased focus on actors. Understanding actors remains central to deterrence. Hybrid actors still have goals, motivations and vulnerabilities that can be discerned and exploited to inform a deterrence strategy. The more an actor can be understood, the more tailored and effective deterrence measures will be.

4.3.4. Respond. This component addresses how to respond to hybrid threats or attacks when deterrence has failed. The decision to respond by implementing appropriate actions and measures can be taken at any stage in the hybrid threat cycle, from the identification of potential vulnerabilities that require resilience-building activity to measures taken in response to a specific hybrid attack. Every response to hybrid threats is shaped first and foremost by the tailored strategic goals of the defending actor to which the response must contribute. Going "beyond deterrence" to respond assertively to hybrid threats could be crucial to changing the behaviour of hybrid adversaries. The response should be well orchestrated and coordinated within all of Government Domains. While hybrid threats are designed to hamper or prevent decisive responses and countermeasures, there are viable ways to respond assertively and move "beyond deterrence".

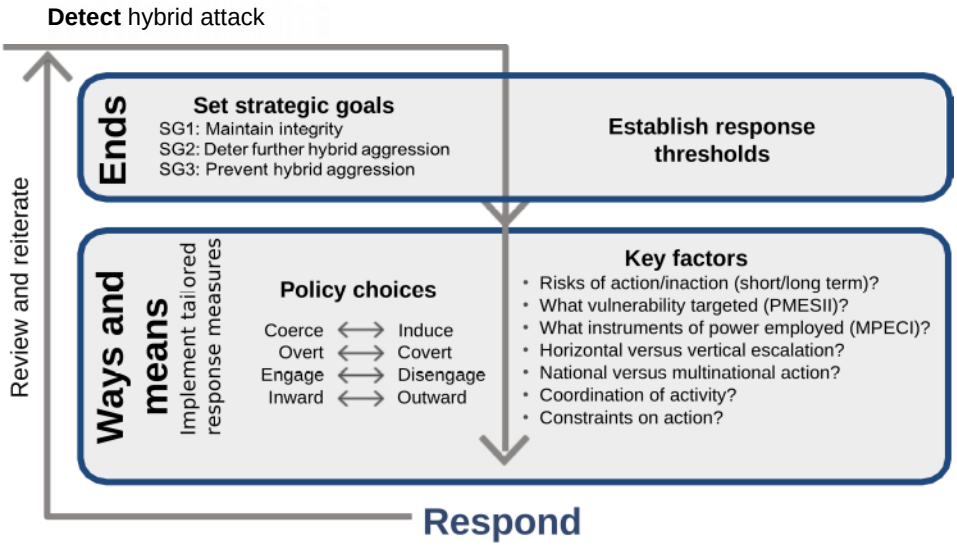


Figure 4. – The countering hybrid threats response framework

- Ends. Not every hybrid attack may require a response. If a response is necessary, the "ends" (what outcome the response should achieve or contribute to achieving) are set according to the tailored strategic goals and thresholds for action of the responding actor. These should be kept under continuous review to make sure they are appropriate and achievable.

  - Set the strategic goals. If the capacity for independent action (SG1) can be maintained despite an attack – for example where resilience measures already in place could help absorb or withstand attack – then it may be appropriate to take no response. More demanding strategic goals will require more decisive action to deter aggression (SG2) or prevent further attacks (SG3).

  - Establish response thresholds. Governments cannot respond to every incident of hybrid activity. Thresholds for response must therefore be

established based on what level of hostility can be reasonably tolerated. Each strategic goal requires a threshold or set of criteria to determine when to respond to achieve each goal. Setting thresholds that take into account why and when to respond to hybrid threats ensures responses are justified, appropriate and consistent.

- Ways and means. Once it has been decided that a response to hybrid aggression is appropriate and the ends have been established, the next step is to identify the specific "ways" and "means" that might be employed to achieve the ends. These should be formed by considering policy choices, key factors and instruments of power.

  - Policy choices. Every response to hybrid threats is shaped first by the tailored strategic goals of the defending actor to which the response must contribute. There are four main "policy choices" in a response. These policy choices are interdependent and not mutually exclusive: elements of all of them may feature in some responses. Taken together they define the character of the response.

    a) Engage versus disengage.

    1) An engagement policy that confronts hostile hybrid activity, for example by exposing and attributing cyber-attacks, can provide effective deterrence.

    2) A disengagement policy that simply ignores or dismisses an attack as irrelevant or inconsequential can contribute towards preventing its recurrence by denying the adversary the intended effects (such as media coverage).

    b) Inward versus outward.

    1) In some cases, the response will be entirely inward-focused, for example, in educating our population about disinformation.

    2) In other cases, the response will be outward-focused towards the adversary, for example, through private diplomatic channels.

    c) Overt versus covert.

    1) Overt action could be classified as public, obvious and official. It can be targeted inward and outward, and can be effective in generating public awareness and support, or exposing adversary action and intent to a wide audience.

    2) Covert action can be classified as having a limited audience, being subdued and even deniable. It can be effective in sending direct messages to adversary decision-makers and having direct physical effects that can deter or prevent an adversary from conducting further hybrid attacks.

    d) Coerce versus induce.

    1) Coercive measures should seek to exploit the benefits of creative horizontal escalation through credible and creative low-level measures targeted across PMESII vulnerabilities using the MPECI instruments of power that impose costs to create coercive effect.

2) Inducement is the attempt to change adversarial behaviour through positive incentives. It can often lead to successful behavioural change by itself or when it complements coercion.

3) Risks: While the risk of coercion is inadvertent vertical escalation, the risk of inducement is the perception of weakness - which could also lead to inadvertent escalation.

- **Key factors**. The following key factors are elements to take into account when assessing the policy choices, before selecting and tailoring the measures to be taken in response to a hybrid attack.

  - Risk. Plans need to consider the risks of taking action versus the risks of not taking action in response to a hybrid attack. All actions have consequences in the short- and longer-term: while the short-term risk of action might be minor escalation, the longer-term risk of inaction might be major escalation by the adversary.

  - Vulnerability. Plans must consider our own and the adversary's PMESII vulnerabilities. For inward resilience measures, the vulnerabilities targeted will belong to us; while for outward responses, the adversary's vulnerabilities will be targeted.

  - Instruments of power. Plans must consider what MPECI instruments of power will be employed. The instruments of power should provide the opportunity to influence the targeted vulnerabilities.

  - Horizontal versus vertical escalation. A response to a hybrid attack may also exploit the benefits of coordinated horizontal and vertical escalation (see Figure 5). It shows how a hybrid actor can synchronize its MPECI instruments of power to escalate vertically and horizontally a series of specific activities to create effects. It also shows how a hybrid actor can either vertically escalate by increasing the intensity of one or many of the instruments of power, and/or horizontally "escalate" through synchronizing multiple instruments of power to create effects greater than through vertical escalation alone. While a hybrid adversary does this to remain under response thresholds and generate complexity, the responder may benefit in the following ways:

    a) Manage escalation through proportionate responses.

    b) Manage escalation through asymmetric responses.

    c) Increase the target "surface area" through targeting a wider range of vulnerabilities.

    d) Pursue low-level responses through horizontal escalation that are more credible because they are easier to implement.

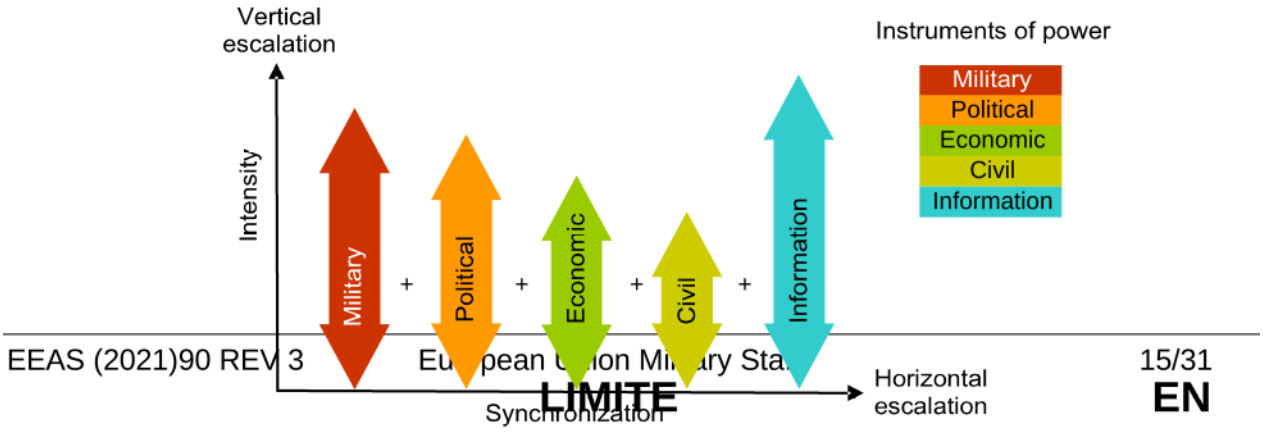


Figure 5. Using the Analytical Framework to consider horizontal and vertical escalation in response to hybrid attack

- National and multinational action. Plans should consider whether the response involves national or multinational activity. A multinational response can provide more varied and effective responses and beneficial second-order effects (such as the perception of solidarity), but can be more difficult to plan, generate and implement.
- Coordination. Any action to respond to hybrid aggression should be coordinated both within national government and society (through dedicated organizational machinery), and between nations where appropriate (through multinational frameworks).
- Constraints. The legal basis for responding to hybrid attacks must be clear, as one of the defining characteristics of hybrid attacks is the exploitation of legal "grey areas". Yet international law allows for an evolving range of responses to a variety of aggressive or hostile activity[3].

5. Planning military operations and missions

5.1. Within military operations and missions, Armed Forces need to be fit to execute military Command and Control (C2) of their respective unit whilst simultaneously acting in a shared (and not lead) engagement space (real as well as virtual) amongst and with civilian authorities. Therefore, trust and co-operation must be developed when the threat allows. Particularly important is inter-agency[4] planning and leadership through influence, advice and informal followership is built upon standing individual networks and relationships.

5.2. The plans need to focus on longer-term activities that may take place many years in advance of the aims and objectives of an adversary becoming obvious and yet they need to be able to respond to shocks and surprises that may quickly lead to a fait accompli being achieved. The plans and planners need to be highly agile and adaptive yet robust and modern.

5.3. Critical dependencies within plans also need to be understood. An adversary will be seeking to understand where our critical dependencies are and how they can undermine our operational effectiveness by attacking these dependencies. Robust teaming of a plan should ensure that these vulnerabilities are identified, and mitigations sought, particularly if time is available.

[3] United Nations Article 51 and UN Security Council Chapter 7 action or countering hybrid aggression without requiring the use of force: sanctions, financial protection, capacity building, security sector reform, anti-corruption, resource diversification, education, infrastructure protection, cyber defence, soft power or media regulation.

[4] It is cooperation where two or more agencies, from different sectors that hardly relate to each other, cooperate to achieve joint outcome.

5.4. The integrated approach[5] is the best for countering Hybrid threats and increasingly should become the normal way of working for planners faced with operating in this complex environment. When it comes to providing a solution to a problem, a military solution may not be the best as civilian organisations may have greater expertise, resources and capacity to resolve an issue. In a comprehensive response, military planners should look to conduct information exchange with non-military organisations in order to achieve information fusion that will be of benefit to all. Here, military may have a great deal to offer due to their expertise in the principles of information fusion and C2 capabilities, although it might be some difficulties in fusing civilian information in to a common picture.

5.5. It is important during planning for operations in a hybrid environment that as broad a view as possible is taken in to account. This will ensure that as many possibilities are covered and that different perspectives on what might happen are considered. This is because this is what any adversary is doing in seeking the obscure fracture line that has not been considered. At every level of military operations different hybrid events could occur, each with the potential to have strategic consequences if not anticipated or dealt with quickly once they emerge. Therefore, each level of planning needs to identify any hybrid threats and opportunities when they conduct their planning.

5.6. Planning staffs at the EU level need to be prepared to integrate other organisations into their process, while respecting the principles of inclusiveness and decision-making autonomy. Ideally, this will have been identified and rehearsed beforehand to make the integration easier. The military contribution to a hybrid warfare plan needs to understand the relationships with other organisations; are they supported or supporting? This will help frame relationships and ease any frictions that may arise. Planners should also expect personnel from other organisations to have no understanding of the planning process or to conduct a process that may be considerably different.

5.7. Under a multi-agency [6] approach, the termination criteria and cessation of a conflict can be better understood and achieved. A multi-agency approach will be key to anticipating this and identifying where and when this is likely to happen or has happened. Measuring performance and effectiveness using traditional military tools may prove challenging. Using a multi-agency approach to inform those tools will undoubtedly make understanding effectiveness and performance easier.

5.8. Success in a hybrid environment is incredibly difficult to determine. This is due to the inherent characteristics of a hybrid warfare event. An adversary may cease activity in a particular sphere only to increase it in another. Therefore, it should be assumed that hybrid warfare will always be present, it will ebb, and flow as required to achieve ends. Success does not look like beating an adversary but more like forcing them to cease a particular activity but recognising that they may engage in another in pursuit of their aims. Planning staff needs to be aware of this and prepared to cease a particular activity in order to pursue another one. This may call for a dynamic response from them and consequently a less polished product.

5.9. In hybrid warfare, the aim is to get an adversary to desist from their activity. Beating them or achieving success in a conventional sense is highly unlikely given the nature of hybrid warfare. Traditional methods or theories of success must make room for different approaches. The ends may be achievable through a variety of means that do not produce catastrophic effects on any population as this needs to be avoided if

[5] An approach, which brings together Member States, relevant EU institutions and other international and regional partners, as well as civil society organisations (multi-lateral) and should be ensured at every level of military command.

[6] An approach, which involves several different organizations that work together for a shared aim.

possible due to the second and third order consequences. In essence, it is best to adopt a plan that will allow opportunities for a hybrid actor to cease their activity and return to normal relationships with as little loss of face as possible.

5.10. Planners also need to be prepared for the hybrid actor(s) rapidly changing its strategy in response to our actions. This may be ceasing activities, but it is important that we can continuously monitor the environment to ensure that we detect when our responses are having an effect and we can scale back or increase activity in different areas of the PMESII spectrum to keep the pressure up on a hybrid actor(s). Effects used should be aimed to influence behaviours not necessarily destroy, in the first instance.

6. Adaptation of the planning process

The difficulty in discovering hybrid threats, due to the multiple levers of power used by the actors and their ability to rapidly adjust their ways and means, presents a unique challenge about how to detect hybrid threats activity.

6.1. Therefore, some recommendations for general rationale and considerations as well as the key questions and actions that planners may want to consider before the challenging of the hybrid threats should be taken into account during the different phases of the military strategic planning process (see Annex A).

7. Adaptation of the planning tools

7.1. There are several tools that complement the planning process for military operations and missions. Analytical tools, such as Centre of Gravity (CoG) analysis, Comprehensive Preparation of the Operating Environment (CPOE), operations assessments, and risk evaluation all assist critical thinking regarding specific portions of the planning process. Knowledge management tools, such as synchronization matrixes and information collection plans facilitate the processing of vast amounts of information, as well as the representation of key deductions, comparisons, and conclusions to others.

7.2. Existing military planning tools and processes remain applicable in a hybrid environment. However, they may need to undergo slight modifications to be more aligned with specific characteristics of hybrid environment. Many of these tools and processes are already designed and employed within a comprehensive approach to operations and missions, including the need to work collaboratively with non-military stakeholders.

7.3. In some cases, modifying these tools for a counter-hybrid approach will apply equally. Each of the tools will benefit from greater collaboration, for instance. In other cases, modifications may apply more to one group of tools than another. As with most aspects of a counter-hybrid approach there is no generic solution commanders and staffs are encouraged to think creatively about adapted solutions.

7.4. Analytical Tools

7.4.1. This category of tools assists in the detailed examination of specific topics, often by breaking that topic into smaller parts. CoG analysis, for example, identifies an actor's principal source of power by looking at critical capabilities, critical vulnerabilities, and critical requirements. For these tools to be effective, planners must be able to draw upon a solid base of knowledge, as well as an understanding about how characteristics of hybrid warfare may affect application of that knowledge.

7.4.2. Traditional CoG analysis has focused on the identification of fixed, primarily military, CoGs. In a counter-hybrid approach, hybrid adversaries may have multiple, relevant, non-military CoGs. Furthermore, priorities may shift among

them in a flexible and dynamic manner. This will have clear impacts on the development of operational designs, likely increasing the need for flexibility and adaptability. Therefore, to remain useful, CoG analysis may need to be modified to incorporate this characteristic of hybrid warfare.

7.4.3. The use of analytical tools must be conducted with an awareness of how new technologies have increased both the possibilities for hybrid action, but also the numbers of potential actors. In a hybrid context, it is possible that the manifestation of power may differ from traditional experiences, with relational power displacing resource-based power as an indicator of influence. Thinking critically about these developments in the operating environment, and how they affect application of these analytical tools will be a necessary step to ensure success of operation/mission plans.

7.5. Knowledge Management and Situational Awareness Tools

7.5.1. These categories of tools, which help collect, assess, and share information, are affected not only by aspects of hybrid activities, but also by developments in the information environment. There is a greater amount of information available, and the primary actors in the information environment are changing. There is also a greater amount of disinformation, which people and organizations are generally less capable of spotting.

7.5.2. Given the dynamic nature of hybrid activities, knowledge management and situational awareness tools must have built-in resilience and flexibility to be able to rapidly identify opportunities in a changing operating environment. Therefore, it may be necessary to amend Synchronization Matrixes to include greater degrees of uncertainty, where activities after certain times are indicated as possible, but not definite.

8. Impact on preparing and conducting military operations and missions

8.1. Operating in a hybrid environment challenges the defence and security status quo since it involves the adversarial use of both new and existing means to target societal functions in innovative ways. Hybrid activities may incorporate deception or disinformation, and they are likely designed to fall below thresholds of detection, making individual hybrid actions difficult to understand. These hybrid activities may involve a wider range of actors than are traditionally considered by the military instrument of power. Combined, these characteristics of hybrid warfare can push personnel and military organizations out of their traditional comfort zones, and, ultimately, stymie potential responses. Additionally, there is possibility that adversary'sinformation operations, social media and disinformation can target individual soldiers and their private life, outside AOO/MAA is not excluded too.

8.2. A principle characteristic of hybrid threats is their ability to exploit ambiguity and detection thresholds, creating uncertainty and reducing the ability of friendly organizations to understand the problem and make appropriate decisions. For personnel trained within a traditional, one-dimensional approach to military, or conventional military-related threat activities, this can be particularly frustrating.

8.3. The ability of hybrid threats to exploit uncertainty can exacerbate some of the characteristics of traditional military domains of operations and corresponding organizational structures that emphasize hierarchical, vertical flows of work, centralized decision-making and strict adherence to standard operating procedures. To mitigate informational stovepipes, sluggish communications, and delayed decisions, commanders and staff may need to consider alternatives to traditional organizational design, taking due account of the characteristics of the cross-cutting cyberspace and information domain of operations.

8.4. Considering that hybrid adversaries can escalate their activities horizontally and vertically in different domains, effective military counter-hybrid strategies must be synchronized with and comfortable at integrating with other instruments of power. To accomplish this, organizational structures must be designed in a manner that promotes horizontal integration with other military and civilian actors. This structure may be on a permanent or ad hoc basis, and either it may be a combination of traditional hierarchical chains-of-command and more non-traditional matrixed or networked work team. In either case, the organizational design must be done in a manner that avoids informational stovepipes and contributes to the development of shared situational awareness and understanding across not only the military instrument, but with other stakeholders.

8.5. Flexibility and adaptability will be necessary components of any effective counter-hybrid strategy given the tendency for shocks, surprises, and innovation by hybrid competitors and adversaries. However, for a counter-hybrid strategy that includes adaptability to succeed, it must be reinforced with a match in organizational culture. Therefore, to prepare for a counter-hybrid campaign, commanders and staff should consider how to ingrain flexibility and responsiveness of thought and deed into the culture of their organizations.

8.6. One of the principles of deterring a hybrid adversary is resilience, which, while intended in a governmental and societal manner, applies equally to organizational structures and the people within them. At the individual level, resilience is a function of how quickly and completely personnel can recover from severe stress, whether short-term crises or long-term challenges. Individual resilience may be enabled by multiple sources, including personal psychological characteristics such as a positive attitude and cognitive flexibility, as well as physical fitness, and social support. All these components can be positively influenced by commanders and staff, either by modelling appropriate behaviour and setting an encouraging cultural tone, or by emphasizing the importance of exercise, a trait that should already be a part of military organizations.

8.7. While individual resilience is important within teams and the overall organization, group resilience is more than the sum of the people. In addition to the components that enable individual resilience, team resilience is also affected by communication, leadership, and shared vision and understanding. Group resilience, whether at the team or organizational level, can also be negatively impacted by additional factors, such as lack of control, interpersonal conflict, or insufficient resources.

8.8. Pre-crisis behaviours that can help augment group resilience includes situational understanding of current readiness, which includes being aware of and communicating personal readiness levels, but also involves the tracking of vulnerabilities, such as resource availability or access to expertise. Another pre-crisis behaviour to increase resilience is the identification of early signs of a crisis, which involves ensuring that warnings are not dismissed prematurely, and that team members can recognize the signs of an emerging problem. Pre-crisis is also the time for commanders and staff to mitigate vulnerabilities, identify back-up responsibilities, and develop standard operating procedures that will carry the organization through a crisis.

8.9. Although a whole-of-government activity, counter-hybrid threats relies mainly on non-military tools. Therefore, forming a counter-hybrid strategy and developing much of the whole of government institutional machinery – the processes, mechanisms, people, and skills needed to synchronize and collaborate across government will largely lie outside the military instrument of power. That said, the military instrument must have input into, as well as a complete understanding of how the strategic approach intends to maintain capacity for independent action, dissuade or deter an

adversary from hybrid aggression, and disrupt or prevent an adversary from taking further hybrid aggression.The military instrument must also provide advice and input into the development of this strategic approach to ensure it is supportable with assigned resources.

Annex A

Recommendations for adaptation of the military planning process

Introduction

The aim of this annex is to help to the planners understand what they should consider at each planning step[7] on countering hybrid threats. These recommendations are not definitive and planners should always look at supplement or enhance it with their own knowledge and experience.

1. Initiation

1.1. Rational and considerations. The Joint Intelligence Preparation of the Operational Environment (JIPOE) and other intelligence products must provide commander and his staff with information about:

1.1.1. The levers of power used by the adversary,

1.1.2. Adversary possible strategy,

1.1.3. The different actors' present in the Area of Operation/Mission area (AOO/MA), the dynamics of relations between them and the coordination already established with them.

1.2. Key questions and actions:

1.2.1. Has the adversary strategy been identified?

1.2.2. Have the levers of power used by the adversary and other actors been identified?

1.2.3. Have all actors' present in the AOO/MA, as well as their dynamics and relationship been identified?

1.2.4. Request, if needed, to the higher level to develop intelligence products to answer these questions.

2. **Initiation - Commander`s initial planning guidance**

2.1. Rational and considerations. The Initial Planning Guide (IPG) and Warning Order (WO) must include at least the adversary's key vulnerabilities and enablers for identified strategy, the ways and means putting a special emphasis on their information operations, its aims in the cognitive domain and the manipulation of international law in its favour.

2.2. Key questions and actions:

2.2.1. Do the IPG and WOs contain the basic information to understand the operational environment and the mission to carry out against the adversary?

2.2.2. Do we correctly understand how the adversary and other actors make use of the cognitive domain, the information functional area and of our perception of the law and traditions?

2.2.3. Has the establishment of the relationships with the different actors ' present in the AOO/MA been authorized?

[7] Initiation, mission analysis, COA development, COA analysis, COA validation and comparison, commander's COA decision and plan development.

3. **Initiation - Liaison and reconnaissance team deployment**

3.1. Rational and considerations. Operational Liaison Reconnaissance Teams (OLRT) must count among its components specialists to discover the levers of powers being used and to be in contact with the different actors present in the AOO/MA.

3.2. Key questions and actions:

3.2.1. Does the OLRT have specialists from the different levers of power capable of contributing to the JIPOE and other intelligence products?

3.2.2. Does the OLRT have negotiation and liaison specialists?

4. **Mission analysis - Strategic context review**

4.1. Rational and considerations. A thorough review and appreciation of the strategic aspects of a situation is needed to set the context for operational activities, and, in turn, to initiate operational level planning. Some of the most important aspects to review in a hybrid environment will include:

4.1.1. Involvement and perceptions of the international community regarding the conflict,

4.1.2. CoG assessment of adversaries and other international stakeholders,

4.1.3. Economic factors,

4.1.4. Applicable international law,

4.1.5. Information activities of different actors,

4.1.6. Assessment about the receptivity and susceptibility of targeted populations to messaging.

4.2. Key questions and actions:

4.2.1. How do different actors and stakeholders perceive the strategic environment and the factors contributing to the situation?

4.2.2. What is the perception of the international community?

4.2.3. Has the adversary's strategy and CoG been identified, to include how the may be synchronizing their instruments of power?

4.2.4. What are the adversary's key vulnerabilities?

4.2.5. Who are the actors and proxies supporting the adversary's strategy?

4.2.6. What is the CoG of other actors and stakeholders?

4.2.7. What are our own key vulnerabilities, and how are they susceptible to the adversary's strategy?

5. **Mission analysis - appreciation and refinement of the JIPOE**

5.1. Rational and considerations. The JIPOE is a primary tool to ensure that situational awareness (SA) is continually updated. Traditional approaches to compiling a JIPOE are challenged in a hybrid environment since hybrid actors will seek to stay below thresholds of detection through unexpected actions and novel tactics. Therefore, the JIPOE must be continually refined and adapted to accommodate hybrid tactics by using innovative methods to reimagine indicator-based warning methodologies, as well as incorporating alternative warning methodologies that move beyond indicators.

5.2. Key questions and actions:

5.2.1. Are all stakeholders regularly updating the JIPOE?

5.2.2. Is the JIPOE being distributed to all stakeholders?

5.2.3. Are the intelligence products constantly examining our own critical vulnerabilities across the PMESII spectrum?

6. **Mission analysis - evaluation of actors**

6.1. Rational and considerations. In a hybrid environment, it is particularly important to have a deep understanding of potential adversaries and other actors. This includes: their goals, strengths and weaknesses, and how they employ their instruments of power, such as military and security forces. Since hybrid adversaries often act in the framework of a network, it is important to analyse the components of this network to understand relationships and influences, possible proxies, and potential supporting activities. In turn, this analysis will help identify strengths and critical vulnerabilities of the hybrid adversary, and this information must be routinely updated in the JIPOE.

6.2. Key questions and actions:

6.2.1. How current and extensive is our understanding of hybrid actors and their potential proxies?

6.2.2. Do we have authorization to engage with different actors to better understand the situation by including their perspective? If not, have we requested direct liaison authority?

7. **Mission analysis - Factor analysis and key factors**

7.1. Rational and considerations. In a hybrid environment, factor analysis must pay particular attention to:

7.1.1. Time. The readiness and authority of decision-makers and available forces to implement countermeasures in response to actions of a hybrid adversary.

7.1.2. Space. The interdependence and overlap of physical and non-physical domains, and how the absence of clear geographical boundaries might affect delineation of the AOO/MA, Area of Influence, and Area of Interest for our Armed Force.

7.1.3. Force / actors. The non-military capabilities available to a hybrid adversary and what effect they might have on military operations and missions, possible hybrid Tactics, Techniques, and Procedures (TTPs), or known limitations that might impact a hybrid adversary's actions, such as legislation, or sociocultural traditions.

7.1.4. Information. The actors involved, what messages they convey, and to what extent they dominate or influence in the information domain. This factor must also consider our own activities in the information domain and possible actions to intervene in order to obtain an advantageous position.

7.2. Key questions and actions:

7.2.1. What is the Notice to Move (NTM) or reaction time of available forces and whole of government actors, and is this enough for the perceived hybrid threat? If not, how can reaction times could be reduced?

7.2.2. Has the AOO/MA and Area of Influence been clearly defined in all domains?

7.2.3. Are there any international laws or generally accepted customs that restrain or / and constrain the actions of a hybrid adversary?

7.2.4. What are a hybrid adversary's capabilities in the information domain and how are they being used?

8. **Mission analysis - Operational objectives and criteria of success**

8.1. Rational and considerations. Given the opaque nature of cause and effect in a hybrid environment, it is particularly important that operational objectives and intended effects are planned to where they will have greatest effect on other actors, such as on their vulnerabilities. This must be matched with a deliberate and disciplined commitment to measure the effectiveness of our actions, which may be through innovative or non-traditional methods.

8.2. Key questions and actions:

8.2.1. Have we considered how our actions will affect the Centre(s) of Gravity of a hybrid adversary or other actors and what consequences this may cause in their employment of their instruments of power?

8.2.2. Are these the effects we want?

9. **Mission analysis - CoG identification and analysis**

9.1. Rational and considerations.

9.1.1. Since the CoGs of all actors in a hybrid environment could change over time, Lines of Operations (LoOs) and Courses of Action (COAs) must be developed with sufficient resilience to plan for and adapt to new COAs, branches, and sequels, both our own and the hybrid adversary's.

9.1.2. When identifying critical capabilities, the analysis should consider:

- How the adversary will act in the cognitive domain, critical infrastructure and its resilience to cyber or physical attacks?
- The adversary's ability to establish and use information networks,
- How current the situational awareness is and how frequently it is updated?
- The ability to communicate and interact with a local population before, during, and after an action(s),
- The capability to respond to a hybrid action(s) in a timely manner, and the ability to interact with partners and allies in an inclusive way for all EU Member States.

9.1.3. When identifying critical vulnerabilities, special attention should be paid to:

- The degree that adversary manipulates information and/or controls the media,
- The possible unlawful use of cyberspace by a hybrid adversary,
- The ability to boost the narrative and actions of citizens and dissident groups within an actor's territory,
- How quickly violations of international law could be exploited?
- The ability to isolate adversary from obtaining critical resources from third countries,
- The use of dual commercial technologies,
- How vulnerable a targeted population may be to an adversary's discourse?
- The degree of societal resilience.

9.2. Key questions and actions:

9.2.1. Does the JIPOE identify areas in which an adversary's CoGs could be affected?

9.2.2. Have we identified how an adversary's CoAs might change due to their CoGs being targeted?

9.2.3. Have the adversary's critical capabilities, in particular those related to no physical domains, been considered?

9.2.4. Have the critical vulnerabilities, in particular those related to non-physical domains, been identified?

9.2.5. Are all the adversary's breaches of the law or/and any actions against population being exploited to isolate them?

10. **Mission analysis - Developing assumptions**

10.1. Rational and considerations. There is often a lack of factual information available to planners in a hybrid environment because of the long-term nature of many hybrid strategies, the indirect approach taken by hybrid adversaries, and the difficulty of attribution. Therefore, planners will need to make frequent use of assumptions, particularly when developing contingency plans. Due to the versatility and creativity of hybrid actors, assumptions should initially be kept as broad and open as possible, preserving as many options as possible and allowing events and actions to develop over time to help develop greater clarity. An updated JIPOE will provide the confirmation or denial of assumptions and help influence decisions to execute branches and sequels.

10.2. Key questions and actions:

10.2.1. Have we confirmed or denied a hybrid adversary's strategy and its use o instruments of power?

10.2.2. Can we in turn confirm a hybrid adversary's CoA?

10.2.3. Is there enough information for the J3 and J5 to plan for and adapt to the evolving operational environment through branch plans and sequels?

11. **Mission analysis - Determining critical operational requirements**

11.1. Rational and considerations.

11.1.1. Since effective counter-hybrid warfare is a whole-of-government activity, it is especially important that all the instruments of power be able to work in coordination. A key enabler of this whole-of-government synchronization is a robust and reliable C2 structure able to reach all stakeholders in any circumstance.

11.1.2. At the same time, it is not enough simply to understand all the relevant actors in an AOO/MA. To develop effective counter-hybrid plans that include a whole-of-government perspective, it is also important to incorporate these other stakeholders from the beginning of the planning process. In particular, planners should seek input from these stakeholders as to how they perceive conditions for success, as well as how they could potentially create effects and set the decisive conditions needed to reach objectives. In this way, the development of LoOs and COAs can lay the framework for the whole-of-government team to work together.

11.1.3. The elements of the information system should be permanently updated with the operational situation at the operational level, and the current conditions in line with the guidelines of the strategic communication.

11.2. Key questions and actions:

11.2.1. Are the C2 arrangements and the supporting communications networks robust and reliable, and they have enough capacity to integrate other partners, while respecting the principles of inclusiveness and decision-making autonomy? Have we considered technical solutions and/or use of liaison officers?

11.2.2. Has liaison been established with other actors in the AOO/MA? Have those actors been integrated into the planning process?

11.2.3. Consider having the media include messages that promote a positive vision of friendly actions, fundamentally focused on achieving, as a minimum, the non-belligerence of the local population.

12. **Mission analysis - Limitations on operational freedom of action**

12.1. Rational and considerations. The limitations and restrictions imposed by the political level and the operation/mission commander must be kept to a minimum, mainly respecting the rule of law and coordination with other levers of power.

12.2. Key questions and actions. Monitor the civilian situation to avoid any actions or measures negatively affecting the local population's perception on our forces and operation/mission.

13. **Mission analysis - Risk assessment and tolerance**

13.1. Rational and considerations. Risk assessment in a hybrid environment is complicated because it must not only consider risk associated with the physical domain, but also with non-physical domains such as cognitive and cyberspace. In addition, risk assessments must consider the second and third order consequences of actions by all the different actors and how these could potentially impact other actors´ vulnerabilities.

13.2. Key questions and actions

13.2.1. Do our COAs take into account the impact of counter-hybrid activities among the local population, and how it effects on the international community?

13.2.2. Does the risk assessment include perspectives and mitigation measures from across the instruments of power?

14. **Development of the initial operations design - Determining lines of operation**

14.1. Rational and considerations

14.1.1. The strategic objectives must provide planners with enough flexibility to allow for the development of LoOs that are creative and agile.

14.1.2. In a hybrid environment, an indirect approach should be used, applying second and third order effects with the aim to attack or influence the adversary in an unexpected and hidden way. To do that, planners might wish to seek marginal gains by focusing on key vulnerabilities, targeting specific assets that enable the hybrid threats or increasing focus on specific sensitive actors.

14.2. Key questions and actions. When designing LoOs and COAs, planners should consider how to achieve marginal gains through disaggregation of a hybrid adversary's strategy and attacking key enablers with the most effective instrument of power.

15. **Development of the initial operations design - Conditions to be established and selection of decisive conditions**

15.1. Rational and considerations

15.1.1. When determining which actions will produce intended effects, it will be important to identify which elements of an adversary's system can be

influenced by military or non-military means. The use of coordinated actions will be important to increase the impact on hybrid actors.

15.1.2. Planners should take into account the possible effects of non-aligned actors in the operating environment and how these might influence the setting of decisive conditions.

15.1.3. The time is a critical factor to study regarding the harmonization of different LoOs, the coordination of simultaneous near and deep operations in the physical and non-physical domains, as well as execution with a high tempo to gain and maintain the initiative.

15.1.4. Due to the ability of hybrid actors to quickly adapt strategies and method of actions, the operational design must be agile and responsive to quick changes. This will put a premium on the need for flexibility in the execution of current operation/mission, as well as on adapting future operations/missions.

15.1.5. Lastly, it is important to consider that in the initial phase of a crisis, if there is no escalation, the main actions may have a dissuasive character.

15.2. Key questions and actions

15.2.1. Has the CoG of any of the actors changed?

15.2.2. Determine which elements of an adversary's system can be influenced by military and / or non-military means.

15.2.3. Has a network been established to coordinate actions with military and non-military actors not embedded in our force?

15.2.4. Have we identified the actors with a supporting role to the military forces? How will they provide this support and what effects they will produce?

16. **Courses of action development - Adversary and opposing non-adversary actors**

16.1. Rational and considerations. Hybrid actors are typically characterized by creativity, agility and dynamic decision-making; they generally have the capability to change strategy, plans and actions to accommodate the ever-changing conditions of the operational environment.

16.2. Key questions and actions:

16.2.1. Evaluation of adversarial courses of action:

- Has it been possible to figure out the adversary strategy?
- Are the indicators established to confirm that the adversary's course of action as valid?
- Are the assumptions, used in planning, to predict the operating environment confirmed?

16.2.2. Evaluation of the actions of non-adversary actors:

- With the available information, can we deduce the actions, the levers of power used, and the actors that produce negative effects for our forces?
- Are the actions of the opposing actors coordinated and, if so, what levers of power do they use?

17. **Courses of action development - Own courses of action**

17.1. Rational and considerations

17.1.1. In a hybrid environment, our own COAs must be as flexible as possible to be able to respond to any change in the situation. This flexibility, along with the integral flexibility of our own military forces, will provide the opportunity to react before using the planning tools of branches and sequels.

17.1.2. Flexibility must also be a factor when integrating with other actors to coordinate actions in a supporting/supported role. In all cases, planners should seek non-linear effects and to coordinate effects using all the instruments of power.

17.1.3. Effective counter-hybrid strategies put a premium on the operation assessment process to check that plans are achieving their intended objectives and, if required, to adapt current operation/mission through branches and sequels. Due to the uncertainty, that characterizes a hybrid environment, the numbers of branches and sequels could be very high, which will put pressure on intelligence information to confirm or deny the indicators.

17.2. Key questions and actions:

17.2.1. Are the COAs flexible enough to adapt quickly to a hybrid adversary?

17.2.2. Are the signposts realistic and sufficient to be able to see changes in the COA of the adversary and enable us to take decisions in a timely manner?

17.2.3. Have the measures of effectiveness been established to see the effects of our actions in one or more orders on the adversary, neutral and friendly actors?

17.2.4. Is there a constant assessment of the results of our COA regarding the objectives at each time and phase of the operation?

17.2.5. Do we have the required RFIs and CCIRs from higher HQs and subordinate units to confirm or discard the branches (J3) and sequels (J3 plans and J5), as well as next future operating environment (J5).

18. **Courses of action analysis - Wargaming**

18.1. Rational and considerations. The wargame must include all the actors present in the AOO/MA, it must be used to confirm the strategy employed by the adversary, and, if necessary, revisit the decisive conditions, actions and effects. Wargaming should also identify the need to plan branch and sequels and serve to define the decisive points that will trigger decisions by a commander.

18.2. Key questions and actions:

18.2.1. After wargaming our own COA against that of the adversary, can we tell if our COA is flexible enough to adapt to the hybrid adversary?

18.2.2. After wargame, have enough indicators been identified to confirm or discard the adversary's COA?

18.2.3. Does our own COA allow us to seize the initiative in non-physical domains, such as in the cognitive and cyberspace domains, and in the information function?

18.2.4. Do we have representative involvement from all whole of government stakeholders in the wargame?

19. **Commander’s course of action decision**

19.1. Rational and considerations

19.1.1. In a hybrid warfare environment, this is a particularly important step as it is where the commander will decide which COA to adopt for subsequent staff development. When presenting information to the commander, a staff must ensure their logic is presented so that the commander fully understands why particular decisions have, or have not, been recommended. Central to all of this is the commander’s own knowledge, including an understanding and acceptance of the hybrid warfare environment and all that it entails. If the commander does not accept the potential impact that hybrid activities could

have on plans or operations, then all the outputs at this stage will, potentially, be skewed away from where the main threats lie.

19.1.2. However, if a commander accepts the potential impact of adversarial hybrid activities on plans and operations, then this will be woven into the outputs of the COA decision process. Whilst planning for operations in a hybrid warfare environment should not require hybrid-specific outputs from this step, the impact of hybrid warfare should be borne in mind throughout so that it is a consideration at all stages of a planning process. When outputs are agreed by the commander, it is important for the staff to ensure that the language used recognises that there is no common, agreed lexicon for hybrid warfare.

20. **Plan Development**

20.1. Rational and considerations

20.1.1. The development of the plan is a key stage where more hybrid warfare factors and critical dependencies that are vulnerable to exploitation by an adversary will almost certainly be uncovered. What is critical at this stage is that the right type of environment should have been established where no one should be afraid to raise an issue at any stage, the consequences of not doing so could be disastrous.

20.1.2. At this stage, the role of enabling capabilities should be considered in more detail. Subject matter experts may come from outside of planning staffs and the use of language will have to be considered so that they are able to clearly understand what is going on and being decided so that they can contribute.

20.1.3. Conflict termination criteria will need to be properly thought through to ensure that they achieve the aim but also do not leave a vacuum of responsibility waiting for someone else to fill it. Although warfighting operations may cease or be complete, hybrid activities may likely persist. What is key here is that this is recognised and prepared for in any plans. Failure to do this will, almost certainly, result in a drawn-out conflict that does not resolve any of the issues but rather adds to the already complicated situation.

20.1.4. In the early phases of any plan, standing or contingency, cognitive manoeuvre will be central to it. Get cognitive manoeuvre right, then there will be little requirement to conduct traditional manoeuvre as the adversary will already be defeated. Certainly, this is what any adversary will be seeking to achieve.

20.1.5. Deployment of military forces to theatre, onwards movement as well as sustaining them is fraught with vulnerabilities. There are numerous vulnerable points created by dependencies on third parties that are vulnerable to outside influences from hostile states; criminality and corruption, either directly or by hostile states using criminals and corruption as their proxies. Equally, protests, strikes or cyber-attacks on to computer systems to confuse manifests could be used against a deploying force. If contractors are used to provide support, then their honesty and reliability could be influenced to ensure that supplies go missing or are not delivered to the correct place.

20.1.6. Joint Fires have an increasingly important role to play in preparing for any conflict. Aside from their traditional role, there should be an increased emphasis on hybrid warfare environments and their impact. It is important to think much more broadly and originally about what could form part of the Joint Fires effect. Here, cognitive dominance as well as cultural

understanding and sensitivity are extremely important in achieving the desired effect.

20.1.7. C2 will also be subject to adaptation during this phase due to hybrid warfare. This is mainly due to the fact that a C2 structure may be imposed upon you and that you will have to adapt to that. Tasks to subordinate formations will also need careful consideration as they will also be operating in a hybrid environment. Direction will need to be carefully considered and co-ordinated in order to ensure that a tactical action does not have a strategic effect.

20.1.8. Rules of Engagement (ROE) are important in a hybrid warfare environment. In such an environment there are plenty of opportunities for adversaries to create issues. Different ROEs between nations can cause friction as social media and the conventional media could be manipulated to create distractions at home.

20.1.9. Information advantage is central to success as it allows achieving and maintaining advantage over adversaries. This is as important in standing plans or contingency ones. Information advantage will allow to conduct proper full spectrum targeting which may now be considerably broader in definition than previously. This will link very closely with Joint Fires.

20.1.10. CIMIC needs to be a proper function as envisaged to be engaging with the local population. It has a central role to play in a hybrid warfare environment and must become more than an afterthought or *"radio in a box"*. Using the correct person in this role, having suitably empowered them may prove to be one the commander's best decisions as this may be pivotal in avoiding direct fight as well as ensuring that as many detectors as possible are employed.

20.1.11. Some Joint Functions will take on an increased importance in a hybrid environment. For example, CBRN is likely to increase in prominence due to the prevalence of toxic industrial materials and hazards and efficacy of biological weapons. Both of these can be legitimately found in environments and as such, their use as a weapon can be relatively anonymous and deniable.

21. **Assessment and Reviewing**

21.1. The very nature of hybrid warfare means that there is a constant requirement to continuously assess and review plans to identify new vulnerabilities and weaknesses in them. Any adversary will continue to seek intelligence, from all quarters, on our plans in order to find those fissures that can be exploited with minimal risk to them and with maximum impact to our forces. Potential faults will naturally appear, particularly if a plan is reliant on technology of a third party to help enable the plan.

21.2. It is important to ensure that the information environment is constantly monitored as well as a continuous assessment of effects is undertaken. This will help in understanding where issues are and what, if anything, needs to be done about them.

21.3. There will also be a continuous requirement to maintain close liaison with higher formations, STRATCOM and psychological operations to ensure that a common understanding is maintained at all times. This will prove vital in providing a common picture to all, which will aid in maintaining up-to-date and coherent plans.

Annex B

Glossary

Ambiguity. Ambiguity is understood as hostile actions that are difficult for a state to identify attribute or publicly define as coercive uses of force. Ambiguity is used to complicate or undermine the decision-making processes of the opponent. It is tailored to make any type of response difficult. It is designed to fall below the threshold of war and to delegitimize or render irrational the ability to respond with the use of military force.

Branches. Branches are options within a particular phase of an operation/mission, which are planned and conducted in response to an anticipated opportunity or risk within that phase, to provide the flexibility to retain the initiative and ultimately achieve the original objective. The planning of branches is sometimes referred to as "contingency planning", which has to be well differentiated from the contingency plan (COP) planning. Branches address the question of "what if?"

Communication. Communication is the two-way understanding and perception that informs cost-benefit calculations on both sides.

Credibility. Credibility is the will to carry out actions that impose costs on the adversary.

Deterrence by denial. Deterrence by denial aims to undermine the ability of the adversary to achieve their objective in the first instance.

Deterrence by punishment. Deterrence by punishment aims to persuade the adversary that the costs of achieving their objective will be prohibitive by threatening retaliation to aggressive action (i.e. sanctions for state hybrid actors).

Discovery of Hybrid threats. Discovery of Hybrid threats involves an attempt to manage the problem of unknown unknowns. This process involves capturing and then correctly interpreting information related to a potentially hostile adversarial action that has not been previously conceived.

Hybrid actor(s). Actor(s) that often employ low-cost, low-risk, and high-reward tactics. They are first movers and use marginal technological advantages, meaning that their activities can be fully under way before they are noticed. They are less restricted by legal and ethical constraints, therefore the broad range of techniques make it difficult to identify and counteract their campaigns

Hybrid threat(s). Mixture of coercive and subversive activities, 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.

Monitoring of Hybrid threats. Monitoring of Hybrid threats involves a process of scanning the environment for known unknowns – usually with the aid of indicators– to look for a set of preconceived information about possible hybrid attacks.

MPECI: Military, political, economic, civil and informational.

PMESII: Political, military, economic, social, information and infrastructure.

Resilience is the ability of society and government to absorb, withstand and recover from disruption and external shocks. Measures to increase resilience contribute to deterrence by denial.

Sequels. Sequels are options for subsequent operations within an operation/mission or the following phase(s) of an operation/mission. They are planned on the basis of the likely outcome of the current operation or phase, to provide the flexibility to retain the initiative and/or enhance operational tempo. Sequels address the question of "what's next?"

Strategic Goal (SG). Strategic goal maintains capacity for independent action. It is also a pre-condition for any subsequent goals.