Paul Tudorache – Ghiță Bârsan[1]

Strategies to Counter Hybrid Threats

Hybrid warfare has been defined in many ways from different perspectives, but for the purpose of this chapter a quite useful definition consists in "synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects".[2] Thus, from the beginning it can be estimated that hybrid warfare is a very complex phenomenon and therefore the action to combat is just as complex, hence very difficult. Without a holistic approach that must cover all essential aspects of hybrid warfare, it will be very difficult for actionable structures and dedicated capabilities to ensure a tailored response. On these coordinates, the fundamental issues that coagulate a generic picture of the reaction needed for countering hybrid warfare or countering hybrid threats comprise highlighting specific strategies used to understand what should be done in such challengeable contexts. These strategies, regardless of their national, regional or international nature, are supported by dedicated instruments, measures and capabilities which can be used based on the principle of joint, interagency, intergovernmental and multinational cooperation. On the other hand, a coherent understanding of the countering hybrid warfare or countering hybrid threats framework requires identifying some key implications at strategic level, as well as giving some planning guidance for the operational and tactical planners.

Conceptual models

To raise awareness and understand the actionable possibilities within the manifestation of hybrid threats or hybrid warfare, the authors highlight some of the models of fighting strategies used by different states and the international security community to ensure a tailored response. Consequently, in the framework of hybrid warfare, both attackers and defenders use a wide range of strategies so that they can achieve desired goals. From a defender's view, specialised sources approach countering hybrid threats (CHT) or countering hybrid warfare strategies

[1] "Nicolae Bălcescu" Land Forces Academy.

[2] MCDC 2017: 3.

DOI: https://doi.org/10.36250/01195_08

(CHW) from three different perspectives such as national, regional and international. In this regard, at the international level, one of the most representative models is the one portrayed in Figure 1 which is also adopted by NATO.

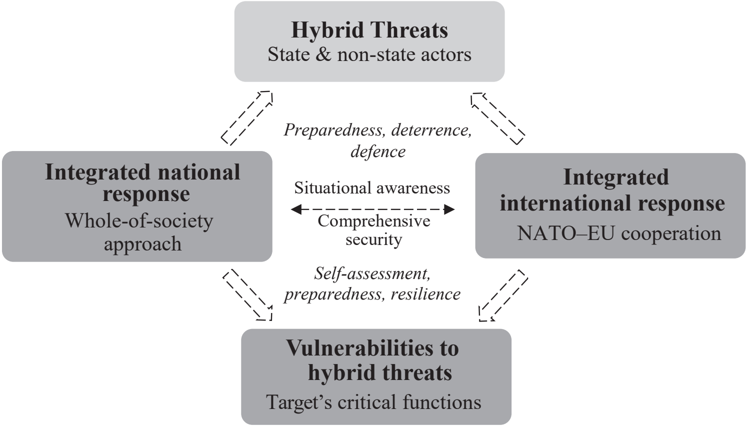
Hybrid Threats
State & non-state actors
Preparedness, deterrence, defence
Integrated national response
Whole-of-society approach
Situational awareness
Comprehensive security
Integrated international response
NATO–EU cooperation
Self-assessment, preparedness, resilience
Vulnerabilities to hybrid threats
Target's critical functions

Figure 1: NATO's conceptual model
Source: Hagelstam 2018

To understand the model above it is necessary to think comprehensively which assumes integrating all necessary capabilities involving both national and international commitments. Specifically, the model indicates that a coherent and timely response requires not only strategies developed against aggressors such as preparedness, deterrence and defence, but also strategies for identifying and diminishing national vulnerabilities such as self-assessment, preparation and resilience. Also, if the national response is shaped by the positive involvement of different national authorities and agencies, the international one is tailored by the smooth cooperation between NATO members on the one hand, and between NATO and other national and regional partners such as the EU, on the other hand. Consequently, taking into consideration the conceptual model highlighted, the key strategies used by NATO for CHT/CHW are:[3]

[3] NATO 2022.

- Preparedness – is triggered by the situational awareness using joint intelligence analysis in order to identify the hybrid threat's imprint. It is achieved by developing operational early warning systems, building tailored resilience for national vulnerabilities, educating and training of specialised personnel and structures.
- Deterrence – is focused on determining the adversary to give up his hybrid threat's and hybrid warfare's actions based on the potential consequences such as political isolation, economic sanctions, and so forth; requires not only proper mechanisms for political and military decision-making, but also deployability of tailored capabilities, anywhere and anytime.
- Defence – is manifested by the ability to act/react in a timely and effective manner for CHT/CHW actions. Here decisional flexibility and capabilities' versatility are required.

As has been previously emphasised, currently NATO is working closely with regional institutions such as the EU to improve the synergistic response of CHT/CHW. In order to be able to stress the correlations between these two organisations, Figure 2 highlights the EU's conceptual model which is currently used.

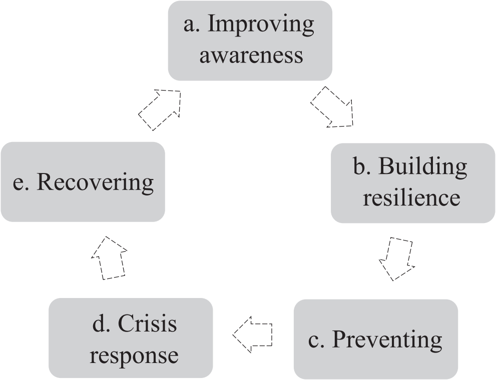

Figure 2: EU strategies
Source: European Commission 2016: 3

As it can be seen in Figure 2, the EU response is based on correlating five dedicated strategies, as follow:[4]

- Improving awareness – is performed by timely exchange of intelligence products between member states in order to recognise the potential hybrid warfare or hybrid threat activities. This strategy is performed by the activity of hybrid Fusion Cell from the Intelligence and Situation Centre, which facilitates the multi-source analyse on the one hand, and on the other hand by the EU Centre of Excellence for Countering Hybrid Threats that conducts specific researches and organises different level exercises.
- Building resilience – is understood as the capacity to resist and recover from hybrid threats or hybrid warfare actions. It is shaped by protecting critical vulnerabilities of energy networks, transport and supply security, space infrastructure, defence capabilities, public health and food security, cybersecurity; moreover, targeting hybrid threat financing, countering radicalisation and extremism or increasing cooperation with partnered countries are other measures taken by the EU to boost its societal resilience.
- Preventing – is done through the capacity of response institutions to preempt hybrid threats or hybrid warfare imprints. It ensures early warning of defensive capabilities to be prepared in the event of hybrid attacks.
- Crisis response – is the actual reaction to hybrid aggression provided by the integrated use of national and European capabilities coordinated by the European Emergency Response Coordination Centre.
- Recovering – is comprised of a set of post-incident measures taken to restore the optimal operating parameters of the attacked infrastructure.

Facing the same hybrid challenges, the EU and NATO cooperate closely in different areas such as situational awareness, crisis prevention and crisis response. From this reason it can be said that the strategies belonging to these two organisations are somewhat correlated. Another model of CHT/CHW, that is somewhat similar in terms of specific phases, is the one designed by the Multinational Capability Development Campaign (MCDC) whose framework is highlighted in Figure 3.

[4] European Commission 2016: 4–16.

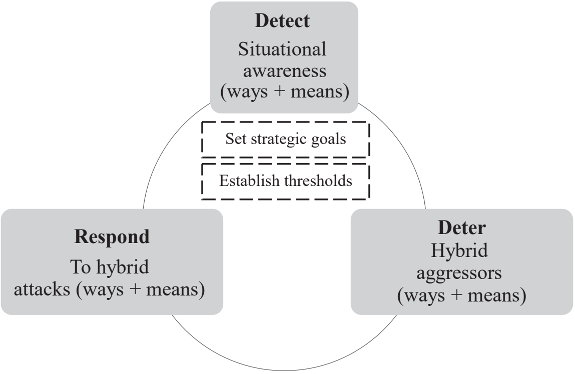
Detect
Situational awareness (ways + means)
Set strategic goals
Establish thresholds
Respond
To hybrid attacks (ways + means)
Deter
Hybrid aggressors (ways + means)

Figure 3: MCDC framework
Source: MCDC 2019: 22

Broadly speaking, the MCDC principles for CHT/CHW to establish the ends called the desired end state in the form of strategic goals based on setting thresholds on the one hand, and on the other hand, to apply specific ways and means within each strategy (detect, deter, respond). More specifically, the constituent elements of the MCDC framework refer to:

- Strategic goals – what is intended to be achieved through countering hybrid threats or hybrid warfare actions (defender's level of ambition). It is settled at the beginning of the hybrid campaign, these are pointed at: independent action capacity, dissuade/deter hybrid attacks and disrupt/prevent hybrid attacks.[5]
- Thresholds – is the hostility level to which countering hybrid threats or hybrid warfare actions must be applied; are correlated with national vulnerabilities and cover political, military, economic, social, infrastructure and information domains as outlined in the previous chapter.[6]
- Detect – is the strategy that focuses on identifying the hybrid threats or attacks through warning intelligence and situational awareness. It can be acquired by monitoring represented by known unknowns or discovery represented by unknown unknowns.[7]

[5] MCDC 2019: 19–20.
[6] MCDC 2019: 90.
[7] MCDC 2019: 26.

- Deter – core strategy for countering hybrid threats or hybrid warfare framework, due to the fact that it is directed at preventing hybrid aggressions; can be achieved through denial deterrence or punishment deterrence.[8] If denial deterrence consists in "[showing] the hostile actor that one can easily absorb the attack with minimal costs to the state that is the target of the hybrid activity",[9] punishment deterrence refers "to threaten to impose costs that are higher than the perceived benefits of aggression, so the hostile actor decides not to pursue the intended action".[10]
- Respond – strategy aiming to calibrate and direct actions using the model of 'ends', 'ways' and 'means' in which coerce/induce, overt/covert, engage/disengage, inward/outward are included.[11]

A more practical perspective regarding the use of the above elements is highlighted in Figure 4 and, as can be seen, the CHT/CHW model is based on 'being in the attacker's mind' principle (in Figure 4, left bold arrow).

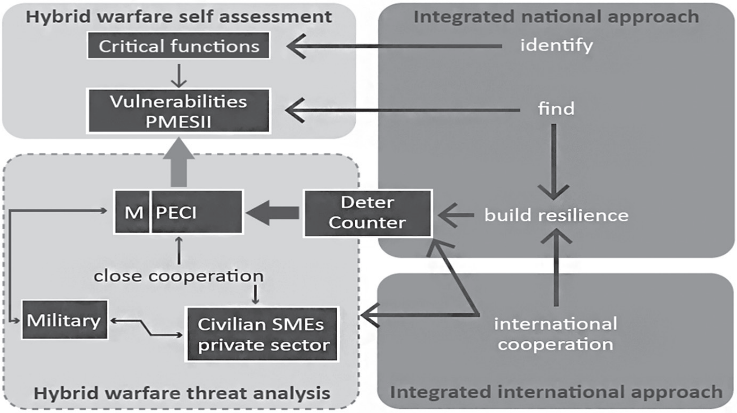
Hybrid warfare self assessment
Critical functions
Vulnerabilities PMESII
Integrated national approach
identify
find
build resilience
M
PECI
Deter Counter
close cooperation
Military
Civilian SMEs private sector
Hybrid warfare threat analysis
international cooperation
Integrated international approach

Figure 4: MCDC conceptual model for CHT/CHW
Source: MCDC 2017: 23

[8] MCDC 2019: 35.
[9] Kersanskas 2020: 11.
[10] Kersanskas 2020: 12.
[11] MCDC 2019: 53.

Moreover, the logical algorithm of the MCDC model's applicability starts with conducting a hybrid warfare threat analysis, covering military, political, economic, civilian and informational (MPECI) fields, and continues with hybrid warfare self-assessment for identifying political, military, economic, social, infrastructure (PMESII) vulnerabilities as well as critical functions, these being used to obtain the desired degree of resilience (involves national and international approach). The algorithm is completed by deterring and responding to the aggressor's MPECI using suitable strategies and capabilities.

Concluding at the end of this subchapter, we can appreciate the fact that the strategies described within CHT/CHW models share similarities as well as some differences. Also, the presented strategies are not the only ones, and others can be added, such as cooperation, persuasion, protection, coercion, control (CPPCC), each of these having specific forms as follow:[12]

- Cooperation – entanglement, conciliation, accommodation
- Persuasion – inducement, assurance
- Protection – defence, resilience
- Coercion – compellance, deterrence
- Control – prevention, pre-emption

Instruments and measures

The applicability of the existing CHT/CHW strategies is achieved by coordinating and directing specific instruments, measures and capabilities. Regardless of the hybrid threat or hybrid warfare nature, there is a common sense regarding the principles of using CHT/CHW instruments and capabilities that are equally transposed on the strategic, operational and tactical framework. These principles, also called joint, interagency, intergovernmental, multinational (JIIM), refer to the following:[13]

- Joint – entities belonging to the same agency/ministry
- Interagency – entities belonging to different agencies/ministries
- Intergovernmental – entities belonging to different governments
- Multinational – entities within different nations

[12] Sweijs et al. 2021: 6.

[13] Wide et al. 2011: 4.

In relation to the intensity of hybrid threats or hybrid warfare, these principles can be fully manifested, situation in which the approach becomes JIIM. On the other hand, any other combinations of these principles are quite possible. Also, analysing the applicability of JIIM to each CHT/CHW level such as the tactical, the operational and the strategic, it can be seen that all principles can be used, either independently or in a correlated manner. However, if at the tactical level the 'joint' principle is more widely used, at the operational and strategic levels, the 'interagency' and 'intergovernmental' principles are more suitable. Instead, the 'multinational' imprint can be recognised regardless of the level in question. As for the instruments used for CHT/CHW, they must be correlated with the domains from which the operational capabilities originate. Thus, the literature review identifies the MPECI and diplomatic, information, military, economic, legal (DIMEL) as specific tools or power instruments. The last one, DIMEL can be used in an extended formula, including other domains such as finance and intelligence (DIMEFIL). Within any hybrid operational environment, "when these elements are 'weaponized' the instruments of power can become tools of [response]".[14] For the MCDC model of CHT/CHW as displayed in Figure 4, the MPECI instruments are used to engage vertically and horizontally the aggressor's PMESII vulnerabilities. Thus, the MPECI can be used not only by the attacker, but also by the defender as a response to hybrid threat and hybrid warfare. If vertical escalation is defined by the intensity of the means employed to deter and repel the hybrid aggression, the horizontal one covers the MPECI domains from which the response capabilities will be ensured.[15] In this regard, the defender may correlate both forms of escalations such as vertical and horizontal, which materialises in a synchronised use of the MPECI capabilities whose direction will generate a tailored intensity. As the authors pointed out at the beginning of this subchapter, another effective tool for CHT/CHW identified in the international literature, is DIMEL/DIMEFIL. The principle of its use is somewhat similar to the MPECI tool, because the DIMEL/DIMEFIL instruments are also used for horizontal escalation as seen in Figure 5. Comparing with MPECI, the aspect of differentiation that appears in Figure 4 5 is based on the detailed description of the response intensity in terms of vertical escalation in

[14] MCDC 2019: 90.

[15] MCDC 2017: 9.

the form of different strategies used as displayed by CPPCC. Considering the volatile, uncertain, complex and ambiguous (VUCA) character of the hybrid threat or hybrid warfare, a correlated use of vertical and horizontal escalation is required to ensure the most comprehensive response.[16]

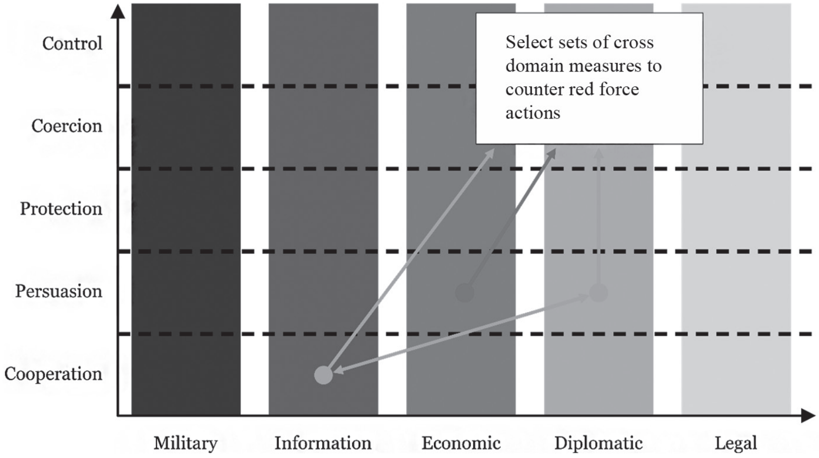

Figure 5: Vertical and horizontal escalation within CHW–DIMEL–CPPCC tool
Source: Sweijs et al. 2021: 7

Another important aspect that needs to be clarified refers to the measures taken for CHT/CHW in relation to power instruments and strategies identified. In this regard, keeping an eye on Figure 5 the authors will focus on identifying specific measures for CPPCC strategies at the level of each domain of DIMEL. Therefore, some measures that can be applied in the CHT/CHW framework are stressed in Table 1 as below. These could be obtained by correlating empirical research based on observation mostly in the form of personal experience with the analysis of specialised sources.

[16] Sweijs et al. 2021: 23–24.

Table 1: CHT/CHW measures – DIMEL and CPPCC tool

Diplomatic		
Cooperation		
Entanglement – building common norms, partnerships, diplomatic channels between public and private sector	*Conciliation* – using neutral parties for mediation	*Accommodation* – empathising with diplomatic issues from different sides
Persuasion		
Inducement – using economic stimulants for diplomatic purposes	*Assurance* – pledging or building peacetime conditions or dissolving wartime organisations	
Protection		
Defence – building or boosting defensive organisations	*Resilience* – using means of public diplomacy to develop national and international diplomatic resilience	
Coercion		
Compellance – threatening with diplomatic isolation to change the subject actor's behaviour	*Deterrence* – threatening with diplomatic isolation to maintain the subject actor's behaviour	
Control		
Pre-emption – expulsion of subject actor's diplomats as well as limiting or prohibiting his access to different international diplomatic organisations	*Prevention* – obtaining the support of various states from the subject actor's neighbourhood and using them to discourage his intention to launch hostile actions	
Information		
Cooperation		
Entanglement – stimulating media activity and identifying journalists from the subject actor's media institutions		
Persuasion		
Inducement – accommodation of the subject actor's propaganda on own territory, provided they will not promote overt misinformation	*Assurance* – ensuring the destruction of sensitive information that discredits the subject actor	
Protection		
Defence – countering various forms of information warfare using media infrastructure and strategic communication	*Resilience* – improving digital literacy and critical thinking to manage the information warfare and implicitly fake news	

Coercion		
Compellance – threatening the subject actor with the use of information warfare's forms to change his strategy; propaganda, misinformation and disclosure of sensitive information may be included	*Deterrence* – threatening the subject actor with information warfare retaliation to discourage changes in his strategy	
Control		
Pre-emption – using information warfare's means to disrupt the subject actor prior to his aggression/attack	*Prevention* – using large scale information operations (fake news, trolls) to discourage the subject actor before direct confrontation	
Military		
Cooperation		
Entanglement – risk sharing regarding the employment of military capabilities	*Conciliation* – promoting arms control activities in order to limit or prohibit the possession and use of dangerous weapons such as Weapons of Mass Destruction (WMD)	*Accommodation* – removing military capabilities from the subject actor's sphere of influence
Persuasion		
Inducement – carrying out arms trade activities to generate behavioural changes of the subject actor	*Assurance* – planning and conducting different military exercises including the subject actor in order to make him aware of own peaceful intent	
Protection		
Defence – developing and revolutionising military defensive capabilities in order to ensure countering the subject actor's attack	*Resilience* – ensuring the operation of military systems and capabilities even when some components are affected or do not function properly	
Coercion		
Compellance – threatening the subject actor with military invasion by prepositioning military forces	*Deterrence* – threatening the subject actor with the use of overwhelming military response capability	
Control		
Pre-emption – launching pre-emptive kinetic or non-kinetic strikes against the subject actor	*Prevention* – launching surgical strikes against the subject actor's high value targets (HVT) in order to diminish his combat power capacity	

Economic		
Cooperation		
Entanglement – increasing mutual economic dependencies	*Conciliation* – facilitating foreign economic competition in the respective markets by reducing or removing various taxes	*Accommodation* – recognising the subject actor as an economic competitor and accepting his presence in one's own economy
Persuasion		
Inducement – accepting the reduction or elimination of debts with the condition of changing current policy	*Assurance* – providing financial and other types of donations to adjust the behaviour of the subject actor	
Protection		
Defence – strengthening energy and supply infrastructure to limit the effects generated by the subject actor's actions	*Resilience* – building various economic connections so that the dependence on singular sources is considerably diminished	
Coercion		
Compellance – threatening the subject actor with the use of economic sanctions to shape his current behaviour	*Deterrence* – threatening the subject actor with the use of economic sanctions to maintain his current behaviour	
Control		
Pre-emption – blocking the subject actor's access to necessary resources for planning and conducting desired attacks	*Prevention* – using large scale economic sanctions to limit/prohibit the development of high-technology weapons systems	
Legal		
Cooperation		
Entanglement – active legal involvement in the various multilateral treaties	*Conciliation* – admitting different perspectives on interpreting the same law to encourage multilateral acceptance	*Accommodation* – expressing agreement related to some deviations from legal provisions
Persuasion		
Inducement – promising to consider the subject actor's opinion when drafting new laws, rules or taking legal decisions	*Assurance* – manifesting leniency towards the subject actor who violates the law to encourage his integration from a legal perspective	
Protection		
Defence – developing legal framework and identifying punitive measures applicable to those who violate the law	*Resilience* – supporting legal framework with new norms to consolidate legal defence	

Coercion	
Compellance – threatening the subject actor with using legal sanctions to determine him to respect the law	*Deterrence* – threatening the subject actor with using legal sanctions to discourage him to break the law
Control	
Pre-emption – withdrawing from different treaties to facilitate national control and autonomy	*Prevention* – prohibiting the manufacture of certain weapons systems

Source: Sweijs et al. 2021: 27–41

These measures are only a few and, as can be seen, they are generic in fashion with applicability, particularly, at the strategic level of CHT/CHW. Regardless of the level, the measures will be applied in a correlated manner, assuming the active participation of different structures, entities and capabilities within each DIMEL domain. If at the strategic level, the degree of capabilities' correlation is greatly amplified, at lower levels such as operational and tactical it decreases significantly, but it is still present.

Strategic level implications

Certainly, a comprehensive understanding of the CHT/CHW also requires deciphering the strategic picture as well as its implications for the operational and tactical levels. In this regard, from the beginning, it is necessary to emphasise the connection between these levels, which can be summarised in the fact that the strategic level should answer the question of How. This level is the one that establishes the methods of response to hybrid threats or hybrid warfare by integrating different strategies and instruments, while the operational and tactical levels are the ones that ensure the application of strategic decisions by accomplishing different missions and tasks using organic capabilities. Therefore, the implications of the strategic level can be reflected on setting the specific goals and thresholds, as well as on selecting the strategies to be used in the CHT/CHW actions. According to the MCDC framework as depicted in Figure 3, all measures and actions should be carried out in such a way as to contribute to the achievement of the following strategic goals:[17]

[17] MCDC 2019: 19–20.

- Preserving the capacity for independent action – refers to maintaining the actionable capacity of all state entities involved in the CHT/CHW effort; being a prerequisite of other additional goals, it largely depends on building and developing resilience in all spheres of society.
- Dissuading/deterring the opponent's aggression – can be reflected in the form of a response with a significantly amplified level of countering, because it means more than denial deterrence, seeking to obtain punishment deterrence if the situation calls for it.
- Disrupting/preventing the opponent from a follow up aggression – is the most complex and demanding due to the fact that it aims to degrade/disrupt the opponent's combat capabilities.

Depending on the footprint and evolution of the hybrid aggression's dynamics, one or more of the highlighted strategic goals can be pursued even within the same operational context. Selecting the appropriate thresholds is another aspect which must be analysed in order to understand the strategic picture of the CHT/CHW. This operation calls for reporting to established strategic goals because "thresholds must be set according to what level of hostility can be reasonably tolerated and what level requires countering"[18] on the one hand, and "hybrid aggressors purposefully target their adversaries by operating below known or perceived response thresholds to avoid decisive retaliation"[19] on the other hand. Consequently, thresholds are indispensable for determining the amplitude of the hybrid aggression and for directing decision-makers when they need to take specific measures in the hybrid warfare framework. Regarding the last aspect of this subchapter, the strategies that can be used for CHT/CHW have been highlighted in the presentation of the conceptual models in the first subchapter. However, some additional information can be related to the selection of the strategies and in this regard, respecting the progressive principle, as appropriate strategies are selected in relation to the identified strategic goals and established thresholds. On the other hand, returning to the influence of the strategic level on the other levels that bring their input to the CHT/CHW, as we have seen, the strategic level is the one at which the desired end state is defined in the form of strategic goals, responsive thresholds and selection/correlation of the strategies necessary for counteraction. Instead, the operational level of CHT/CHW, based on the strategic inputs, is responsible for planning,

[18] MCDC 2019: 21.

[19] MCDC 2019: 22.

coordinating and conducting the actual operations so that multi-domain combat power is directed to the decisive place and time. At the same time, it provides the bridge between the strategic and tactical level of CHT/CHW. The lowest level, such as the tactical level, ensures the implementation of organic capabilities relative to the intent of the operational level, so that, regardless of the hybrid aggression nature, it is combated.

Guidance for operational and tactical planners

At the operational and tactical level, one of the most important activities in managing hybrid threat or hybrid warfare challenges consists in performing tailored planning whose applicability ensures timely and effective countermeasures. For multi-echelon commanders, such as operational and tactical, the operational art and operations design are the most demanding challenges, including the performing of the military decision-making process (MDMP) in all its steps, which constitutes a real obstacle for tactical staff, which can only be overcome by means of detailed adaptive planning. The latter, properly correlated with the commander's conceptual planning, can ensure the achievement of desired end state. Understood as the "cognitive approach by commanders and staff – supported by their skill, knowledge, experience, creativity, and judgment – to develop strategies, campaigns, and operations to organize and employ [capabilities] by integrating ends, ways, and means",[20] the operational art has specific elements including "end state and conditions, [COG], decisive points, lines of operations and lines of effort, tempo, phasing, culmination, operational reach, basing and risk".[21] Also, its applicability is supported by the operations design that focuses on "understanding the situation and the problem".[22] Interpolating their elements, it is found that the centre of gravity (COG) represents an essential ingredient of both, which, addressed in the context of hybrid warfare offers the most significant mutations, of course, by comparing with its determination in the framework of traditional warfare. Considering critical vulnerabilities, requirements and capabilities, the comparative analysis of determining the COG for hybrid warfare and traditional warfare highlights that in the context of traditional warfare the

[20] Department of the Army 2019a: xii.

[21] Department of the Army 2019b: 2–6.

[22] Department of the Army 2019a: xii.

COG bears the imprint of a single source, usually correlated with elements of military combat power, unlike the hybrid warfare framework, where a multitude of power's sources can be identified, which, generally, are not related only to the elements of military power as seen in Figure 6.

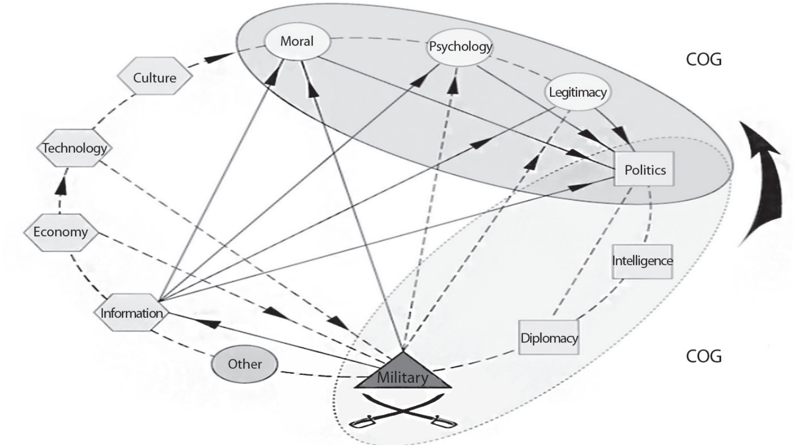

Figure 6: COG in the framework of hybrid warfare
Source: Schmid 2020: 570–579

Moreover, in the hybrid warfare framework, both attacker and defender may use multiple, correlated and shifting COGs that will be flexible, adaptable and dynamic in fashion during a multi-domain confrontation. Besides these, other aspects which commanders and their staff should take into account when planning the operations design may consist in:[23]

- Establishing the ends, ways and means in such a way that they do not follow the overwhelming of the opponent but rather generate a series of interconnected effects, even of the second and third order, which are primarily intended to control the aggressor's behaviour through lethal and nonlethal actions.
- Developing a common operational picture (COP) based on a multi-domain understanding of all significant aspects covering not only the actual subject audiences (sensitivities, perceptions, etc.), but also the different types

[23] MCDC 2020: 42–47.

of interconnections that can be established between them; determining the COGs for all interest audiences should be required.

- Defining the conditions of desired end state so that to be accepted by all interest audiences regardless of their initial perceptions; restoring the critical infrastructure and living facilities should be included.
- Engaging targeted COGs using an indirect approach built on correlating, synchronising and directing the power instruments (MPECI) against targets vulnerabilities (PMESII); the indirect approach should be used to deter and undermine the attacker's hybrid aggression.
- Synchronising the power instruments for each line of operation of CHT/CHW framework; in turn, the lines of operations must be synchronised with each other.

As the authors pointed out earlier, the challenges of countering the various forms of hybrid threat and hybrid warfare can also be encountered at the tactical level, stemming largely from detailed planning. In this sense, during the MDMP, which is a planning methodology used "to understand the situation and mission; develop, analyse, and compare courses of action [COA]; decide on the [COA] that best accomplishes the mission; and produce an order for execution",[24] planners have to adjust each dedicated step according to the hybrid threat or hybrid warfare characteristics and demands. Within each step, these adjustments are given by the following aspects:[25]

- Step 1 (receipt of mission) – by using the two forms of tactical planning, the mission can be received from higher level directly through an operations order (OPORD) in which the planning is subsequent, or through a warning order (WARNO), in which the planning becomes parallel in fashion. Regardless of the planning form, hierarchical documents must provide critical information about the hybrid adversary, including the power instruments such as MPECI, potential strategies, dynamics of relationships with other audiences which are present in the designated area of operations (AO). Also, the higher joint intelligence preparation of the operational environment (JIPOE) should include information on adversary's vulnerabilities, key enablers and different ways/means used within the estimated strategies that can be employed; moreover, to generate an

[24] Department of the Army 2019b: 2–6.

[25] MCDC 2020: 48–61.

effective COP, which is an essential requirement of understanding the hybrid situation, the establishment and use of liaison officers or liaison teams is recommended to facilitate JIIM cooperation.

- Step 2 (mission analysis) – if the first step was to focus on understanding the generic picture of the hybrid operation, this step allows for a more detailed understanding of the situation, as well as the identification of the tactical problem to be solved. In this regard, using JIPOE products and performing the intelligence preparation of the battlefield (IPB), the S2 staff evaluates the adversary and other target audiences, determines their COGs and COAs, and identifies the priority information requirements (PIR). Speaking about the audiences' assessment, including the adversary, determining their motivations, estimating their strength and will to fight, as well as the modalities regarding the use of MPECI instruments, will contribute to visualising the strengths and weaknesses of the hybrid adversary. At the same time, S3 staff must define the key factors of the hybrid operation, determine the friendly forces' COG, develop assumptions, determine the key operational requirements, identify the constraints of the operational freedom of action, develop the initial operations design and so forth. Although each of these requirements has specific features, the S3 staff should pay special attention to the operations design, as it must include multi-domain non-military means.
- Step 3 (COA development) – COA development for friendly forces must start from the premise of being aware of the possibility of continuous change in the COAs of the adversary and of other target audiences, considering the accentuated VUCA characteristics of the hybrid AO. Therefore, friendly forces' COAs must be developed in such a way as to provide a high degree of flexibility necessary to counter any changes that may occur in the hybrid AO, in general, and with regard to adversary's COAs, in particular. Also, this can be supported by a quite flexible operations design and commander's intent, as well as by a high adjustable decisive, shaping and sustaining operations.
- Step 4 (COA analysis) – using the principle of action–reaction–counteraction, this step is performed to examine each friendly forces' COA in order to identify specific advantages and disadvantages. As the authors highlighted, the hybrid footprint of the operation calls for developing the

COAs for all interest audiences that are present in the designated AO and, on these considerations, during war-gaming, not only the friendly forces and adversary's COAs, but also those of the other interest audiences should be simulated. Even if the operational picture increases significantly in its complexity, the advantage of simulating all COAs provide the possibility of estimating the likely effects of other operational audiences on friendly and adversary's COAs.

- Step 5 (COA comparison) – with the aim of identifying the COA with the highest probability of success, this step does not make many adjustments from the perspective of the hybrid operation. Even so, planners must use, in addition to the established comparison criteria (combat functions), and others such as those related to the influence of the indigenous population or the contribution of various civilian agencies, etc. Also, even COAs that have achieved lower probability of success may represent solutions in adjusting the execution to the requirements of the hybrid adversary.
- Step 6 (COA approval) – given the hybrid nature of the operation, the commander's decision should be based on the approval of that COA which enjoys the most conclusive support of friendly forces by multi-domain means, which is due to the fact that combating the hybrid adversary requires the employment of the most diversified capabilities.
- Step 7 (orders production) – once the COA was selected and the concept of operations (CONOPS) approved, planners move on with OPORD's production. It must comprise all critical information that will guide organic and subordinate capabilities to perform CHT/CHW tasks without constraining their freedom of action. On the other hand, the OPORD must give necessary information for all actionable capabilities to protect their critical vulnerabilities.

These are just a few of the many recommendations that planners should consider when dealing with planning operations for countering hybrid adversaries. At the same time, they not only imprint the methodologies specific to operational planning or characteristic of tactical structures with organic headquarters, but are also perpetuated at the level of troop leading procedures (TLP), constituting the planning methodology of the smallest tactical structures such as platoon and company.

Conclusion

Countering hybrid threat or hybrid warfare is the reaction of defenders to hybrid aggression or hybrid attack using multiple strategies, supported by tailored instruments, measures and capabilities, correlated and directed based on the applicability of JIIM principles. The purpose of this chapter is to provide a generic picture that is suitable for national, regional and international defenders. Subchapter *Conceptual models* provides, comparatively, the main conceptual models of countering hybrid threat or hybrid warfare, as well as the strategies underlying them. The main conceptual models analysed in the subchapter are those developed by NATO, EU and MCDC. The NATO model promotes key strategies such as preparedness, deterrence and defence, the EU model strategies consisting in improving awareness, building resilience, preventing, crisis response and recovering, while the MCDC boils down to strategies as detect, deter, respond. Other strategies that may be used in countering hybrid threat or hybrid warfare framework are CPPCC. Subchapter *Instruments and measures* highlights the main instruments and measures that underlie the applicability of countering hybrid threat or hybrid warfare strategies. Within it are explained not only the principles of using MPECI and DIMEL/DIMEFIL instruments in the hybrid framework, but also the main measures specific to DIMEL and CPPCC tool. Subchapter *Strategic level implications* portrays the key implications at the strategic level by setting strategic goals and specific thresholds, as well as selecting/correlating the strategies necessary for counteraction. Moreover, this subchapter defines the relationship between strategic, operational and tactical levels of countering hybrid threat or hybrid warfare. Subchapter *Guidance for operational and tactical planners* provides useful guidance for operational and tactical planners from the perspective of planning a countering hybrid operation. During it, aspects that reflect on the operational art and operations design (COG), as well as on the MDMP are highlighted.

Questions

1. Explain the conceptual models of CHT/CHW used by NATO and MCDC, highlighting the role of constituent strategies and specific elements!

2. What are the main instruments used in CHT/CHW framework to support specific strategies? Identify some CHT/CHW measures using DIMEL and CPPCC tool!
3. What are the main strategic implications in the CHT/CHW framework?
4. Exemplify some measures to facilitate the adaptation of planners to the requirements of the hybrid operation from the perspective of operations design and MDMP!

References

Department of the Army (2019a): *Joint Publication 3-0. Joint Operations.* Online: https://irp.fas.org/doddir/dod/jp3_0.pdf

Department of the Army (2019b): *ADP 3-0. Operations.* Online: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18010-ADP_3-0-000-WEB-2.pdf

European Commission (2016): *Joint Framework on Countering Hybrid Threats. A European Union Response.* Joint Communication to the European Parliament and the Council. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

Hagelstam, Axel (2018): *Cooperating to Counter Hybrid Threats.* Online: www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html

Kersanskas, Vytautas (2020): *Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats.* Helsinki: The European Centre of Excellence for Countering Hybrid Threats. Online: www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf

MCDC (2017): *Understanding Hybrid Warfare.* Multinational Capability Development Campaign. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

MCDC (2019): *Countering Hybrid Warfare Project: Countering Hybrid Warfare.* Multinational Capability Development Campaign. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

MCDC (2020): *Countering Hybrid Warfare 3: Guidance for Planners.* Multinational Capability Development Campaign. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1037061/MCDC_Countereing_Hybrid_Warfare.pdf

NATO (2022): *NATO's Response to Hybrid Threats.* Online: www.nato.int/cps/en/natohq/topics_156338.htm

Schmid, Johann (2020): The Archetype of Hybrid Warfare. Hybrid Warfare vs. Military-Centric Warfare. *Österreichische Militärische Zeitschrift,* 212(5), 570–579.

Sweijs, Tim – Zilincik, Samuel – Bekkers, Frank – Meessen, Rick (2021): *A Framework for Cross-Domain Strategies Against Hybrid Threats.* The Hague: HCSS Security. Online: https://euhybnet.eu/wp-content/uploads/2021/06/Framework-for-Cross-Domain-Strategies-against-Hybrid-Threats.pdf

Wide, Markel M. – Leonard, Henry A. – Lynch, Charlotte – Panis, Christina – Schirmer, Peter – Sims, Carra S. (2011): *Developing U.S. Army Officers' Capabilities for Joint, Interagency, Intergovernmental and Multinational Environments.* Santa Monica: Rand. Online: www.rand.org/pubs/monographs/MG990.html