Paul Tudorache – Ghiță Bârsan[1]

Designing Adversary Hybrid COAs

Different state and non-state actors use a wide range of strategies to take advantage of the opportunities ensured by hybrid warfare (HW). Regardless of the nature of escalation (vertical, horizontal), the adversary correlates instruments of power from the military, political, economic, civilian and information spheres, in a way that generates a non-linear direction, creating an ambiguous pattern, which is quite difficult to decipher and counter. Consequently, this non-linearity of hybrid aggression/attack (HA) requires an exhaustive analysis to be discerned. Starting from the idea that hybrid threats (HT) represent "force multipliers and/or a coercion tactic used to support a policy or strategy that is not delivering the desired results"[2] this chapter seeks to analyse the most representative conceptual models for understanding the framework of HT, as well as to determine a common denominator of the adversary's strategies, operations and tactics. These will be used to substantiate the design of the adversary's courses of action (COA) in the framework of HW. Furthermore, due to the fact that the most acute lethal effects of HA are felt at the lowest level of operations, a comprehensive approach to the various COAs that may be used by the adversary at tactical level of HW is required.

Conceptual models

The principle underlying the desired visualisation and understanding of the overall image of HT/HA requires, first of all, reporting to the representative conceptual models, which analysed and correlated accordingly, will provide the essential generic aspects, constituting a starting point in designing various COAs that may be used by the adversary in the HW framework. To eliminate any confusion from the beginning, it is appropriate to emphasise that the two concepts

[1] "Nicolae Bălcescu" Land Forces Academy.

[2] Giannopoulos et al. 2021: 10.

DOI: https://doi.org/10.36250/01236_09

of HT and HW are used interchangeably. Even though HT is considered a hostile intent of a potential aggressor before his HA in the HW framework, both HT and HA are considered principle forms of offensive actions, and thus both can be considered inherent parts of the HW spectrum.[3] Also, other additional information that substantiates the usage of HW, no matter in what form (HT, HA), refers to the following key principles:

- Creating volatility, uncertainty, complexity and ambiguity (VUCA) – if the volatility consists in the high amplitude of the changes in a very short time, the uncertainty is given by the difficulty of predicting the hostile intentions of the hybrid adversary. Instead, the complexity arises from the diversity of domains and tools used to perform HT/HA, while the ambiguity manifests itself through the hidden and plausible negation, which creates real obstacles in understanding decision-making contexts.
- Generating asymmetry – is achieved by relating and leveraging various deceptive strategies and multi-domain instruments and capabilities against expanded target vulnerabilities. In this regard, the synchronisation of the HT/HA usage can be obtained by relating horizontal and vertical escalation of power instruments and tailored strategies.
- Having a multisource pattern – HT/HA can be used by "an actor or a network of actors willing to engage in hostile, usually covert activities […] may be controlled or influenced by a nation-state, proto-state, or a non-state actor such as large organizations, which often attempts to either circumvent or ignore international laws".[4]
- Achieving simultaneous or successive effects – they are multilevel guided, aiming at political, strategic, operational and tactical targets from all fields of societal security to degrade their normal functioning.
- Practising blended tactics – exemplifying at the tactical level, the adversary's operations are based on employing modular conventional military structures reinforced with guerrilla, paramilitary, insurgent or criminal elements.

[3] Monaghan et al. 2019.

[4] Balaban–Mielniczek 2018: 3711.

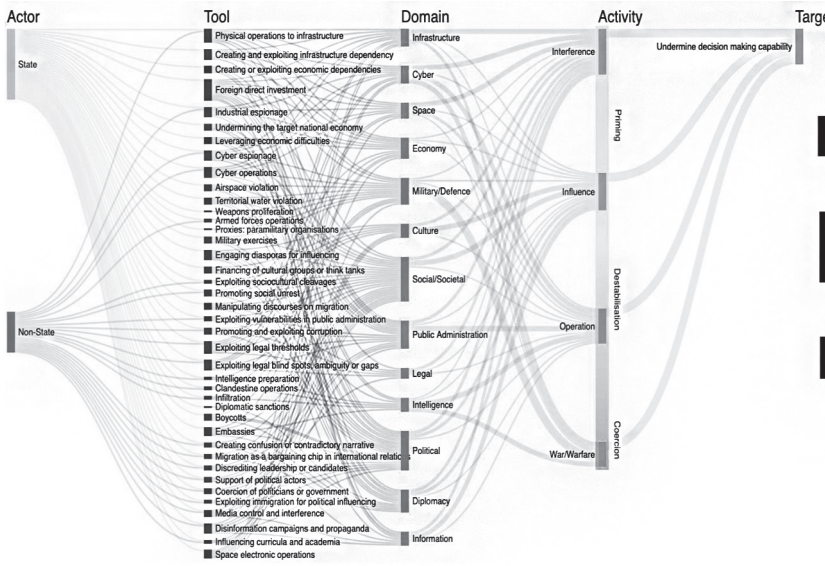

Figure 1: Conceptual model for HT/HA – EU JRC and Hybrid COE
Source: Giannopoulos et al. 2021: 13

A first conceptual model to which the authors refer and which portrays the principles mentioned above is the one developed by the mutual effort of the Center of Excellence (COE) for HW and the Joint Research Center (JRC).[5] As it can be seen in Figure 1, the conceptual model is based on five key elements such as actors, tools, domains, activities and targets. The principle of its operation is quite simple and is based on the progressive correlation of the constituent elements.

The comprehensive understanding of the conceptual model initially involves the proper analysis of each dedicated element. This consists in:

- Actors – can be of two types as state and non-state actors. State actors are considered different countries, which are also found with the name of 'nation-states' and are dominant in the hybrid spectrum. Also, state actors are divided in four main categories as "core states, transition states, rogue states, and failed or failing states".[6] Instead, non-state

[5] Giannopoulos et al. 2021.
[6] Department of the Army 2010: 2-1.

actors are represented by actors that "do not represent the [capabilities] of a particular nation-state […] include rogue actors as well as third-party actors".[7] Insurgents, mercenaries or guerrilla are some examples of rogue actors, while refugees, transnational corporations or news media falls in the category of third-party actors.

- Tools – are defined as "the ways in which an actor might bring about an effect".[8] The effects can propagate not only on one but on several domains, because they are strongly interrelated. For instance 'cyber operations' could impact military, infrastructure, space, public administration domains, while 'diplomatic sanctions' could influence economic, diplomatic or political domains.
- Domains – defines the vulnerabilities or opportunities against which the various tools and activities are directed for their targeting or exploitation; within the model shown in Figure 1, the domains are extremely diversified from infrastructure to diplomacy or information.
- Activities – are used to "harm, undermine or weaken the target"[9] and can manifest, according to the gradual escalation, in various forms such as interference, influence, operation or warfare. These activities are correlated with specific phases, consisting of priming, destabilisation and coercion. First phase, priming, also known as shaping or conditioning phase, can be acquired through interference and influence, destabilisation through operations, while coercion requires warfare strategies and tactics.[10]
- Targets – the objects of the tools and activities undertaken by the aggressor to generate desired effects, either lethal or nonlethal; as can be seen in Figure 2, they are extremely diversified, being correlated with various domains.

Relating to the elements above, the understanding of the conceptual model can be summarised as state or non-state actors, with certain defined objectives, but with a limited capacity of achieving them. They use various tools to engage multi-domain targets in order to create desired effects so that they are affected

[7] Department of the Army 2010: 2-1.
[8] Giannopoulos et al. 2021: 33.
[9] Giannopoulos et al. 2021: 36.
[10] Giannopoulos et al. 2021.

and shaped according to the desired end state. Furthermore, in relation to the aggressor's objectives, the tools will be used, escalating or de-escalating vertically and/or horizontally during priming, destabilisation and coercion phases of the HW. If in the priming phase, the aggressor uses the tools and activities to obtain certain advantages but also to test his own capabilities or to check the defender's readiness. In the stabilisation phase the goal is to achieve a deliberate objective, the use of tools and activities being much more visible and aggressive, thus challenging the limits of their acceptance or non-acceptance by the defender. Instead, in the last phase, coercion, the aggressor moves to the maximum escalation of aggression through the overt and covert use of the entire typology of strategies, tools and activities, resulting in a tailored mixture of military operations, subversive and propaganda activities, political and economic measures and so forth.[11] Another conceptual model, as representative as the previous one, but which portraits the attacker's behaviour depending on that of the defender is shown in Figure 2.

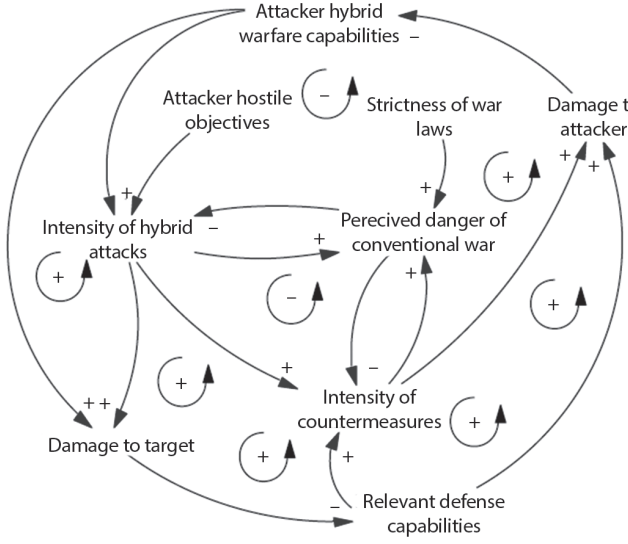

Figure 2: Designing attacker and defender's behaviours during HW
Source: Balaban–Mielniczek 2018: 3714

[11] Giannopoulos et al. 2021.

According to the model, the HA intensity is strongly correlated to the attacker's objectives and fluctuates depending on his HW capabilities. Also, the HA intensity influences in a positive way both the amplitude of the effect on target and the intensity of the defender's reaction. For this reason, it can be concluded that the higher the HA intensity, the more pronounced the effect on target and implicitly the defender's countermeasures will be. Thus, damaging the target through the effects obtained decreases its defensive capabilities, on the one hand, and on the other hand, it stimulates the defender's responsiveness capacity, which in turn limits the attacker's offensive capabilities.[12]

Adversary's tools used

From the information provided, it can be easily inferred that HW is an extremely complex and dynamic phenomenon, in which the opponents can use a wide variety of measures and capabilities to fulfil their objectives. For this reason, the HW is defined as "the synchronized use of multiple instruments […] tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects".[13] Practically, in this framework, the adversary tries to determine and use the most suitable formula for engaging the opponent, which is built using the harmonious integration of different tools such as those in Table 1.

Table 1: Adversary's tools used for HT/HA

Tools	Targeted domains
Kinetic operations against infrastructure	Infrastructure, Cyber, Economy, Space, Military, Information, Social, Public Administration
Building/exploiting economic dependencies	Economy, Political, Diplomacy, Public Administration
Building/exploiting infrastructure dependencies	Infrastructure, Economy, Cyber, Military, Space, Public Administration
Industrial espionage	Economy, Intelligence, Information, Infrastructure, Space, Cyber

[12] Balaban–Mielniczek 2018.

[13] Cullen – Reichborn-Kjennerud 2017: 3.

Tools	Targeted domains
Exploiting economic burdens	Economy, Political, Diplomacy, Public Administration
Undermining the national economy of the target state	Economy, Political, Diplomacy, Public Administration
Cyber operation/espionage	Cyber, Space, Infrastructure, Military, Public Administration
Territorial violation	Military, Political, Diplomacy, Social
Weapons proliferation	Military
Armed forces operations	Military
Rogue and third-party actors' activities	Military, Social
Military exercises	Military, Political, Diplomacy, Social
Supporting cultural groups	Culture, Social, Political, Diplomacy
Shaping/exploiting diasporas for own interest	Diplomacy, Political, Social, Culture, Intelligence
Building social disturbances	Social, Economy, Infrastructure, Political
Exploiting public administration's vulnerabilities	Public Administration, Social, Political
Promoting/exploiting corruption	Social, Public Administration, Legal, Economy
Exploiting law's vulnerabilities	Legal, Infrastructure, Diplomacy, Political, Intelligence, Information, Cyber, Space, Military, Economy, Culture, Social, Public Administration
Intelligence operations	Intelligence, Military
Clandestine operations	Intelligence, Military
Infiltration	Intelligence, Military
Disinformation and propaganda	Information, Political, Cyber, Culture, Social, Public Administration
Media and interference	Information, Social, Culture, Infrastructure
Electronic operations	Cyber, Space, Military, Economy, Infrastructure
Exploiting migration/immigration for political purposes	Social, Political, Diplomacy
Supporting/discrediting political actors/leaders	Political, Social, Public Administration
Coercion of governments/political leaders	Political, Legal, Public Administration
Diplomatic sanctions	Political, Diplomacy, Economy
Using embassies	Diplomacy, Intelligence, Political, Social

Source: Giannopoulos et al. 2021: 33–35.

It should be noted that only a few of the tools that can be used by the adversary for coagulating the HT/HA are scored in the table. Also, visualising these tools, it can be seen that their relationships can form the aggressor's hybrid behaviour, but not every combination of them can be considered hybrid. Normally, the hybrid character is given by the combination of tools from various domains, but here too there are exceptions. For instance, using 'exploiting economic burdens' together with 'undermining national economy of the target state' might not be hybrid, different from 'armed forces operations' combined with 'rogue actors activities' which should be considered hybrid.

Adversary's strategies, operations and tactics

Another aspect that must be clarified within this chapter refers to highlighting some of the strategies, operations and tactics that might be available to the hybrid adversary. All these, correlated with the previous information, substantiate the aggressor's probable COAs. Regarding the hybrid adversary's doctrine, other key principles underlying his aggressive behaviour are given by:[14]

- Centralising the decision-making capability – is achieved by integrating all civil and military decision-makers, necessary to coordinate the hybrid actions.
- Assuming hybrid actions as core missions – involves the adaptation of the traditional doctrine by including the necessity of carrying out missions/tasks in the HW framework.
- Carrying out long-term aggressive information campaigns – necessary to enhance the 'patriotic consciousness' for resurrecting the national fighting will; on the other hand, information operations (IO) are used to generate non-lethal effects on the target state's population and local administration bodies, as well as on the international community.
- Developing the expeditionary capabilities – necessary to achieve conventional strategic deployment and conduct HW actions anywhere and anytime.
- Improving the ability to use private security companies (PSC) or other proxies – in a HW spectrum the aggressor's operational success largely depends on his capacity to use conveniently PSCs or other proxies; by

[14] Clark 2020.

doing this the aggressor will improve his fighting power which will be directed against the defender's vulnerabilities.
- Prioritising the IOs and subordinating the kinetic operations to IOs – if in conventional warfare the lethal operations are more important than IOs, in case of HW contexts we witness a radical change, due to the fact that non-lethal effects are planned and generated more frequently, often proving more effective.

Generally speaking, the strategies that can be employed by an aggressor in HW are complex and multidimensional. According to literature review, a hybrid aggressor may use four types of strategic-level COAs triggered by his strategic objectives. These COAs are briefly described in Table 2.

Table 2: Aggressor's strategic-level COAs in a HW framework

COA type	**Particularities**
COA_1: Strategic operations	conducted for precluding an extraregional power to intervene in an interest region have a continuous character, being used during wartime and peacetime, as well as during the other types of operations (COAs) use all types of power instruments (tools) to engage the defender's centres of gravities (COG) previously use non-military means, and afterwards, depending on the situation, military means primarily target national will, public opinion, political decisions, leaders and warriors' morale
COA_2: Regional operations	directed against regional defenders or internal threats conducted both for countering threats and exploiting opportunities in order to maintain or expand the aggressor's regional influence have a pronounced conventional offensive pattern, aiming to disaggregate the defender's capabilities and diminish his resisting will by engaging armed forces, local population and critical infrastructure, limiting freedom of movement (FOM), destabilising control, retaining initiative, etc. depend on strategic operations in order to preclude an outside intervention
COA_3: Transition operations	directed with dual purpose for retaining the initiative and handling with an outside intervention; thus, are adopted when another actor, regional or extraregional, manifests his intention or actually intervenes in support of the defender used as a bridge between regional operations and adaptive operations, being able to expand in any of the two directions comprise specific elements of regional and adaptive operations

COA type	Particularities
COA_4: Adaptive operations	adopted for preserving the aggressor's combat power, degrading the opponents' fighting capabilities, gaining time for successful strategic operations conducted as a counteraction to the defenders' reaction, especially for countering the additional actor's intervention based on a defensive posture, correlating conventional and unconventional capabilities (last one more presented) to balance the combat power

Source: Department of the Army 2010: 4-1–4-4

All these COAs are sustainable and can be adopted depending on the strategic context, in relation to the defender's reaction and other considerations related to the operational environment. Normally, strategic-level COAs could be adopted successively with the development of the strategic and operational dynamics, which means that the aggressor should start with COA_1 and progressively could reach COA_4. Moreover, as we pointed out before, COA_1 should be correlated with the other COAs, because strategic operations are absolutely necessary for shaping the operational environment. Therefore, there are several options (strategies) regarding the applicability of the proposed COAs, as follows:

- COA_1 – when the aggressor can achieve the desired objectives only through strategic operations.
- $COA_1 + COA_2$ – involves the application of combat power in an offensive manner (mostly likely conventional imprinted) supported by strategic operations to shape the operational environment (shaping operations).
- $COA_1 + COA_2 + COA_3$ – largely similar to the previous version plus the need to counter the intervention of another regional or extraregional opponent.
- $COA_1 + COA_2 + COA_3 + COA_4$ – one of the most complex variants, because it relates to all the proposed COAs. It is almost similar to the previous one to which is added the need to adopt a defensive posture (most likely unconventional imprinted) as a result of the overwhelming combat power of the opponents.
- $COA_1 + COA_2 + COA_3 + COA_2$ – as complex as the previous variant, but in this situation the aggressor returns to regional operations (offensive fashion) due to the fact that he has sufficient combat power to handle with an extra adversary regionally or extraregionally.

Certainly, other strategies in the form of strategic-level COA combinations can be established, for understanding the aggressor's behaviour in the HW framework. Regardless of the selected strategy, the aggressor will contextually combine conventional and unconventional ways and means to fulfil his desired strategic objectives. Within these combined strategic-level COAs, the adversary may use a wide variety of blended tactics to fulfil designated missions and tasks. For instance, at the tactical level these blended tactics allow the adversary to operate both conventionally and unconventionally/asymmetrically. If for conventional activities the adversary normally uses regular and paramilitary forces, for unconventional ones he might use a mixture of elements including insurgents, guerrilla, terrorists, criminals, partisans, gang violence, demonstrations, riots, and so forth. On the other hand, conventional tactical activities are offensive, defensive, stability and enabling in nature, different from asymmetric tactical activities which cover a lot of tasks such as "diversionary actions; reconnaissance and early warning; money laundering, smuggling, transportation; civic actions".[15] Moreover, although each element of the hybrid force is designated to perform specific tasks, in the context of HW regular elements can also be used for asymmetric tasks, just as unconventional elements can be employed for offensive, defensive, stability or enabling tasks.

Hybrid COAs at tactical level

Understanding the previous aspects also involves the tactical design of some possible hybrid adversary's COAs which match the hybrid strategic-level COAs. These COAs will stress the type of operation, elements of combat formation, specific tasks and finally the scheme of manoeuvre (SOM). Each of the three COAs address a theme of major combat operations (MCO), and all will have specific elements of information warfare (INFOWAR). The first COA which fits into the context of strategic-level COA_2 (regional operations) has an offensive imprint and deals with a dispersed attack. From a theoretical perspective, this type of attack is an offensive action adopted when the defender is technologically superior or the aggressor does not have the capacity to provide integrated command and control (C_2) during his offensive operation. In this scenario, the hybrid adversary uses regular military forces and guerrilla elements to fulfil

[15] Department of the Army 2010: 6-7.

his designated mission. Visualising Figure 3, it can be seen that the adversary's combat formation include the following types of forces:[16]

- Fixing/disruption forces – company/battery-level units organised from reconnaissance, antitank, mechanised infantry and multiple launch rocket systems (MLRS), as well as guerrilla and INFOWAR capabilities.
- Assault forces – a detachment including 3 light infantry companies, 2 antitank batteries, 1 air defence artillery (ADA) battery and INFOWAR capabilities.
- Exploitation forces – a combined detachment comprising special purpose forces (SPF) teams, 1 ADA battery, 1 artillery battalion and guerrilla affiliated elements.

Figure 3: Hybrid dispersed attack
Source: Department of the Army 2010: A-4

[16] Department of the Army 2010.

As it can be understood by analysing Figure 3, there are specific tasks that must be conducted by each designed detachment. According to the sketch from Figure 3, these tasks generally refer to:[17]

- Fixing/disruption forces – fix the reconnaissance elements; perform deception, electronic warfare (EW) and IO; limit the use of reserves and quick reaction forces (QRF); neutralise/destroy intelligence, surveillance, reconnaissance (ISR) capabilities
- Assault forces – neutralise C2 and joint fires capabilities from the brigade level
- Exploitation forces – destroy brigade main support and sustain capabilities

Regarding the specific SOM which can be detached within this hypothetical scenario, it is characterised by the following aspects:[18]

- Using fixing forces, the attacker disrupts the defender's brigade capabilities; to do so the attacker generates IO's lethal and nonlethal effects including engaging indigenous population from the urban area of operation (AO), jamming brigade communications (EW), conducts tactical deception with all organic elements including multiple launch rocket system (MLRS) battery to deceive armoured reconnaissance battalion and the two infantry mechanised battalions with the location and time of decisive operation.
- While the deception is conducted by fixing forces, the attacker introduces the air assault detachment to neutralise the brigade C2 using INFOWAR/electronic attack and other kinetic capabilities. At the same time, he destroys the defender's joint fires capabilities.
- Once the assault forces are about to accomplish their tasks, the attacker introduces the exploitation forces to conduct the decisive operation. In this regard, using special purpose forces (SPF) and guerrilla affiliated teams, supported by heavy artillery fire, the attacker destroys the brigade's main capabilities from designated AO.

Next COA which is suitable with strategic-level COA_4 (adaptive operations) is a hybrid retrograde operation, more specifically hybrid delay from subsequent positions in which the adversary uses a mixture of regular and insurgent forces.

[17] Department of the Army 2010.
[18] Department of the Army 2010.

As can be seen in Figure 4, the adversary's combat formation is structured on four main bodies (detachments):[19]

- Disruption forces – platoon-level subunits organised from motorised infantry, insurgent elements (2 platoons for each) and SPF teams.
- Contact forces – an infantry battalion organised as a battle group (BG) structure (3 company-level BGs); as can be noticed, each interdict direction is covered by a company-level BG (infantry and armoured).
- Shielding forces – antitank, artillery and INFOWAR structures, emplaced on each probable avenue of approach.
- Reserve forces – an armoured battalion emplaced in the assembly area (AA). Armoured battalion is minus due to the fact that an organic company reinforces each company-level BG (1 armoured platoon for each infantry company).

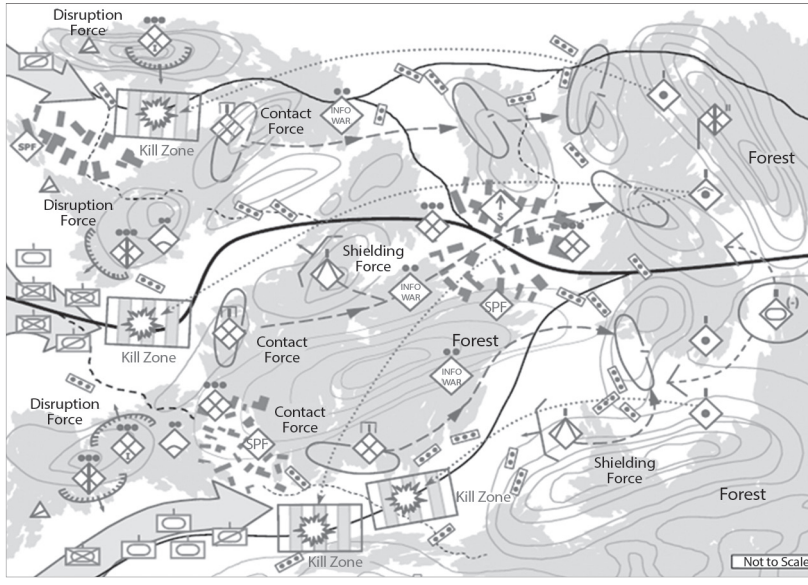

Figure 4: Hybrid delay (from subsequent positions)
Source: Department of the Army 2010

[19] Department of the Army 2010.

On the other hand, each body or detachment has specific tasks, and only their integration ensures the mission fulfilment. More specifically, the tasks may be resumed to:[20]

- Disruption forces – conduct shaping operations for modelling the AO. In this regard, specific tasks are related to fixing the reconnaissance elements that operate on each interdict direction, conducting deception, EW and IO by engaging the indigenous population and local authorities, forcing the premature use of the opponent's main forces, and destroying ISR capabilities.
- Contact forces – engage the opponent's forces during delay by defending subsequently the preplanned battle positions by forcing the opponent's main forces to slow down momentum and to deploy his forces in vulnerable positions (kill zones).
- Shielding forces – support the contact forces with support by fire and jamming communication tasks by fixing the opponent's main forces on interdict directions.
- Reserve forces – conduct the decisive operation by supporting the contact forces in maintaining the battle positions in accordance with the higher echelon's concept of operation (CONOPS).

Correlating all these tasks, the adversary's SOM that can be depicted based on the sketch from Figure 4 has the following form:[21]

- Initially the adversary uses the disruption elements to augment his combat power as follow: engage indigenous population and local authorities using SPF teams; at the same time, using INFOWAR (EW), degrades the opponent's C2 and ISR capabilities by using insurgent and motorised infantry platoons, fixes the opponent's reconnaissance elements and deceives his forces to determine their prematurely operational employment.
- Next, with contact company-level BGs and shielding batteries, defends subsequently the preplanned battle positions in accordance with the higher echelon CONOPS.
- Uses armoured battalion as a reserve to maintain the battle positions and to degrade the opponent's offensive combat power.

[20] Department of the Army 2010.
[21] Department of the Army 2010.

– Finally, using all combat detachments, channels the opponent's main forces in vulnerable positions to create favourable conditions for decisive counterattacks (CATK) conducted by higher echelon using additional combat structures.

Last COA, addressing the theme of stability operations, focuses on correlating guerrilla and SPF actions with passive measures of regular military forces. Related to the strategic picture of the hybrid adversary, this COA can be anchored in the framework of strategic-level COA_3 which deals with transition operations. Because the latter might evolve into two different directions, such as regional operations (strategic-level COA_2) or adaptive operations (strategic-level COA_4), the same could happen in the situation of the current tactical COA (hybrid stability operations). The adversary's combat formation has the following particularities:[22]

– disruption forces – organised from guerrilla elements and SPF teams
– repositioned forces – provided by mixed structures of motorised infantry, mechanised infantry and field artillery

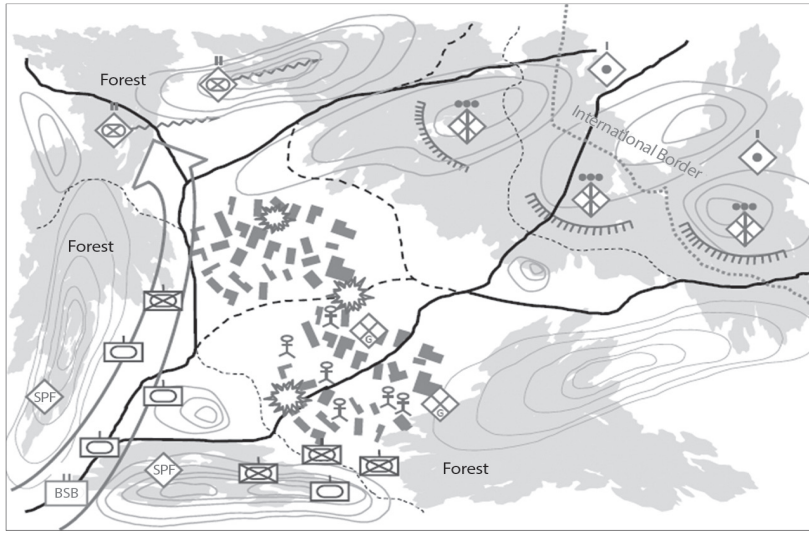

Figure 5: Hybrid stability operations
Source: Department of the Army 2010

[22] Department of the Army 2010.

As far as the specific tasks of the hybrid force's elements are concerned, they are given by:[23]

- disruption forces – fix the reconnaissance elements, deceive the opponent's main forces, conduct EW operations, shape the local population behaviour to gain its support and destabilise civil functions
- repositioned forces – deploy in the preplanned defensive positions in the vicinity of the international border, conduct presence missions in the area with the aim of deterring the opponent

Broadly speaking, the adversary's SOM for this hypothetical scenario is carried out in accordance with the following algorithm:[24]

- deploy regular military forces and occupy preplanned defensive positions
- at the same time, conduct tactical deception using affiliated guerrilla elements and SPF teams such as EW operations, disinformation, sabotage
- use the same elements (guerrilla and SPF) and with the support of indigenous population and local authorities degrades the civil critical infrastructure of the urban AO by conducting kinetic attacks
- conduct deterrence missions through the gradual prepositioning of regular military forces

Within these COAs it can be noted that the indigenous population plays an important role in the outcome of the operations. For this reason and considering the lessons learned from recent/ongoing military operations in Ukraine, Syria, Iraq and so on, the population can support the adversary either willingly or by force, for the latter option being used as a human shield. Also, in order for these tactical COAs to be logical, they must be multi-domain supported at all levels (operational, strategic and political) from a joint interagency, intergovernmental and multinational (JIIM) perspective.

Conclusion

HT and HA are the main fighting forms of HW used by an aggressor opponent. While the HT is considered a hostile intent prior to aggression, the HA represents

[23] Department of the Army 2010.
[24] Department of the Army 2010.

the actual attack using hybrid ways and means. The purpose of this chapter is to generate a comprehensive picture of the adversary's behaviour in the context of HW. Subsection *Conceptual models* highlights some of the representative conceptual models of the HT/HA. Besides the principles underlying them, this subsection analyses the constituent elements of the conceptual models such as actors, tools, domains, activities and targets, as well as the aggressor's behaviour in relation to that of the opponent. Subsection *Adversary's tools used* develops the problem of the tools used by the adversary for coagulating and directing HT/HA. The actual tools within the different domains are highlighted in terms of infrastructure, cyber, economy, space, military, information, social, etc. on the one hand, and on the other hand, the relationships that can be established between them to generate HT/HA. Subsection *Adversary's strategies, operations and tactics* is dedicated to specific strategies, operations and tactics that a hybrid adversary might use to fulfil his objectives. It analyses the main COAs at macro level such as strategic, regional, transitional and adaptive operations, the combination of which forms different strategies used by a hybrid adversary. Also, stressing some of the blended tactics based on correlating conventional and asymmetrical tactical activities is another subject of this subsection. Subsection *Hybrid COAs at tactical level* presents three variants of tactical COAs that might fit in the situation of the hybrid adversary. Within each hybrid COA, the aspects regarding the type of operation, elements of combat formation, specific tasks and SOM are highlighted.

Questions

1. What are the constituent elements of the HT/HA's conceptual models and what is the role of each one? Explain the aggressor's behaviour during HA in relation to the opponent's reaction!
2. What are the tools that the adversary could use for HT/HA?
3. How are the strategic-level COAs applicable to the adversary in the HW framework? Describe briefly each strategic-level COA!
4. Considering the strategic-level COAs, explain some of the strategies that the adversary could use in HW!
5. Explain a tactical COA that the adversary could apply within HW, highlighting the type of operation, elements of combat formation, specific tasks and SOM!

References

Balaban, Mariusz – Mielniczek, Paweł (2018): Hybrid Conflict Modeling. In Rabe, Markus – Juan, Angel A. – Mustafee, Navonil – Skoogh, Anders – Jain, Sanjay – Johansson, Björn (eds.): *Proceedings of the 2018 Winter Simulation Conference.* Gothenburg, Sweden, 3709–3720. Online: https://doi.org/10.1109/WSC.2018.8632492

Clark, Mason (2020): *Russian Hybrid Warfare.* Institute for the Study of War. Online. www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf

Cullen, Patrick J. – Reichborn-Kjennerud, Erik (2017): *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare.* A Multinational Capability Development Campaign. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Department of the Army (2010): *Hybrid Threat. TC 7-100.* Online: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/tc7_100.pdf

Department of the Army (2011): *Opposing Force Tactics. TC 7-100.2.* Online: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/tc7_100x2.pdf

Department of the Army (2015): *Hybrid Threat Force Structure. Organization Guide. TC 7-100.4.* Online: https://irp.fas.org/doddir/army/tc7-100-4.pdf

Giannopoulos, Georgios – Smith, Hanna – Theocharidou, Marianthi eds. (2021): *The Landscape of Hybrid Threats.* Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2760/44985

Monaghan, Sean – Cullen, Patrick – Wegge, Njord (2019): *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare.* A 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