sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXVIII No 1 2022

HYBRID WARFARE — FROM RED TO BLUE OPERATIONAL BEHAVIOURS

Paul TUDORACHE*, Ghiță BÂRSAN, Zoltán JOBBÁGY***, Aurelian RAȚIU***

***"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania**
****"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania,**
Academy of Romanian Scientists, Bucharest, Romania
*****"Ludovika" University of Public Service, Budapest, Hungary**
tudorache.paul@armyacademy.ro, gbarsan@armyacademy.ro,
Jobbagy.Zoltan@uni-nke.hu, aurelian_ratiu@yahoo.com

Abstract: *The manifestation of hybrid actions is not new, but their frequency has increased significantly lately. Nowadays, hybrid warfare is present anytime and everywhere in different forms, and with various degrees of amplitude. Given the fact that hybrid warfare is extremely difficult to decipher, starting with a literature review in the field, the article aims, first of all, to understand the behaviours of different actors from the perspective of their operational strategies. Also, within red and blue strategies identified, the article highlights the main instruments and capabilities used by both attackers and defenders. To fulfil these research objectives, an empirical research based on observation and a comparative analysis will be conducted.*

Keywords: HW, red strategies, blue strategies, MPECI, PMESII

1. Introduction

Analyzing the international and national literature, it can be appreciated that, at present, there are a lot of researches conducted in the field of hybrid warfare (HW). Although most existing researches address issues related to what HW stands for and what its main features are, imprinting different operational areas, especially Ukraine and Russian Federation, not many of them seek to decipher the behaviours of attackers (red strategies) and defenders (blue strategies) during HW manifestation. In this regard, in accordance with the literature review conducted, it has been identified the following relevant aspects:

- Red actors use "*multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects*" [1]; instead blue actors react to HW through setting strategic goals, identifying appropriate thresholds, and implementing specific phases (detect, deter, and respond) [2];
- HW is characterised through "*centrally designed and controlled use of various covert and overt tactics, enacted by military and/or non-military means ... attacker seeks to undermine and destabilise an opponent by applying both coercive and subversive methods*" [3]; defender's strategies may include improving awareness, building resilience, deterring aggression, and responding to attack [4];
- Understanding the actors' behaviours assumes to handle with specific phases from both sides. If aggressor's phases

DOI: 10.2478/kbo-2022-0020

include preparation (political decision), attack, and defending the end state, the defender's phases are integrated in a comprehensive approach based on three specific phases including early warning, hybrid defence and recovery [5].

Even if other reference sources can be identified, it can be considered that the aspects highlighted in the literature review are sufficient to initiate the present research.

2. Research methodology

The purpose of this research is to understand the behaviours adopted during HW manifestations by analysing red-blue dualism. In this direction specific research objectives are:

- Identifying and comparing different operational strategies used by both attackers and defenders;
- Stressing specific instruments and capabilities for red and blue strategies.

The fulfilment of these research objectives requires the applicability of a methodology based on the empirical research based on observation fuelled by a continuous comparative analysis.

3. Understanding attacker's behaviour

In order to stress the behaviours of actors, it is necessary to identify a specific phasing that works either with attackers or defenders in the framework of HW. A useful variant is presented in table 1, covering specific behaviours during HW.

Table1. HW phasing: attacker vs. defender [6]

Attacker		
Political decision	Hybrid attack	Defending the end state
Phase 1: Preparation	Phase 2: Attack	Phase 3: Follow up
Early warning	Hybrid defence	Recovery
Defender		

From the red posture, if in phase 1 attacker's behaviour is somewhat weighted and oriented towards the applicability of multi-domain measures in order to design and shape the environment, in phase 2 the behaviour becomes more offensive because the actual attack really happens, based on attaining the shaping conditions. In the last phase, the behaviour is significantly changed and becomes more defensive in fashion to secure the objectives that have been achieved after the successful hybrid attack.

3.1. Red strategies

As it has been emphasised in the literature review, HW assumes emplacing, in a correlated and orchestrated manner, strategies such as coercion, subversion, conventional, unconventional, using proxies [7], etc. The first one, coercive strategy, is used to put pressure on defenders in a way to determine them to give up fighting and to accept the will and conditions imposed by attackers. The subversive strategy, which is the most preferred by aggressors, includes massive disinformation and other forms such as "*sabotage, disruption of communication and other services including energy supplies*" [8]. If the conventional and unconventional strategies are very well known, using proxy elements or the pretext of humanitarian intervention are other strategies used to destabilise different targeted actors.

3.2. Red instruments and capabilities

The desired behaviours of aggressors can be practiced by making use of full spectrum strategies. Moreover, to generate linear and non-linear effects, the strategies are implemented with the input of specific agents in the form of instruments and capabilities. Regarding the first category, even though there are a lot of classifications of HW instruments, we consider one of the most relevant model the one developed by Multinational Capability Development Campaign (MCDC) according to which specific instruments, including military, political, economic, civilian and informational (MPECI), are used for targeting political, military economic, social, informational, and infrastructure (PMESII) vulnerabilities, vertically and horizontally [9]. Furthermore, from the perspective of HW capabilities, the spectrum is quite wide, because the means cover not only domains from MPECI tool, but also from other additional fields including space, cyber, economy, culture, societal, public administration, legal, intelligence, diplomacy, and so forth.

4. Understanding defender's behaviour

Speaking about defender's posture, in this case the behaviour is quite different from the one adopted by attacker. In the first phase, the behaviour is oriented to recognize all types of HW imprints for operational readiness purposes. Instead, in the next phase the defender's behaviour is coagulated by the timely applicability of tailored measures to respond to the HW attack. For this phase the behaviour could be either defensive (Anti Hybrid Warfare – AHW), offensive (Counter Hybrid Warfare – CHW), or both, depending on the nature of HW imprint [10]. For the last phase, the behavior decreases in its intensity and seeks to rehabilitate the capabilities affected by the HW attack.

4.1. Blue strategies

The need to adopt the appropriate behaviour during HW phases requires defender's decision-making ability to select and adopt the most suitable combination of strategies, covering all phases that characterize HW. Also, as we have pointed earlier, MPECI tool can be applied against defender's PMESII vulnerabilities, vertically and horizontally. In the same way, the defender can respond to the attacker by employing specific strategies to escalate not only vertically, but also horizontally. While vertical escalation assumes using different strategies to direct actions from the same domain as the attacker (red action: cyber attack – blue reaction: cyber defence), the horizontal one differs substantially and consists in applying actions from different domains (red action: military aggression – blue reaction: diplomatic and economic sanctions). Moreover, given the extreme non-linear nature of HW, both forms of escalation will be used in an integrated fashion, simultaneously and/or successively (figure 1).

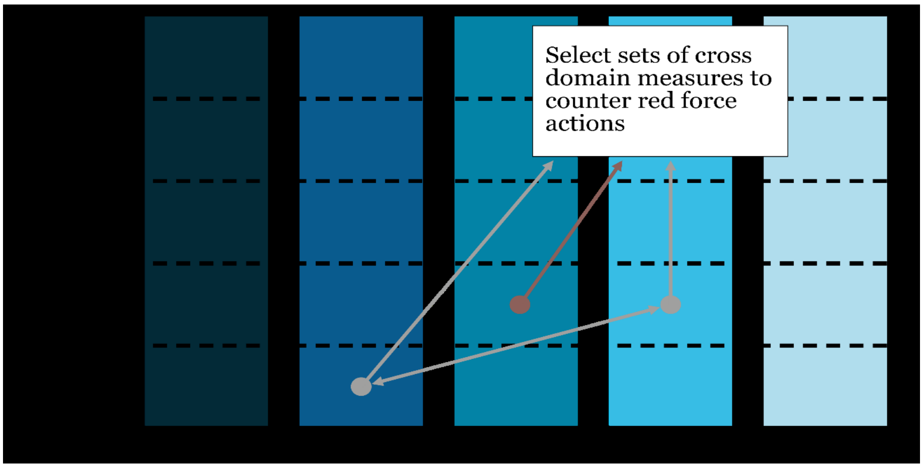
Select sets of cross domain measures to counter red force actions

Figure 1: Defender's response to attacker – vertical & horizontal escalation
Source: Sweijs T, Zilincik S, Bekkers F, Meessen R. A Framework for Cross-Domain Strategies Against Hybrid Threats. Den Haag: HCSS TNO; 2021. Figure 2; p. 7. Available from https://bit.ly/3reuHVJ

Also, as can be seen in figure 1, vertical axis is defined by strategies as cooperation, persuasion, protection, coercion, and control (CPPCC), while the horizontal one works with diplomatic, information, military, economic, and legal (DIMEL) domains. To avoid misunderstandings, the description of CPPCC strategies can be resumed to [11]:

- Cooperation – practicing common beneficial policies to maximize mutual gains for both defender and attacker;
- Persuasion – using different rewards to gain cooperation from attacker's side;
- Protection – setting conditions for defender to resist or absorb the attacker's hostile measures;
- Coercion – making use of different threats to prevent or change the attacker's behavior;
- Control – using force to diminish the attacker's freedom of action (FOA).

Furthermore, a complex and logical model used to understand HW framework is developed by MCDC. From figure 2, it can be seen that its design is substantiated by the principle of 'being in the attacker's mind' (red arrow) in order to identify critical functions, PMESII vulnerabilities, and the most suitable strategies.

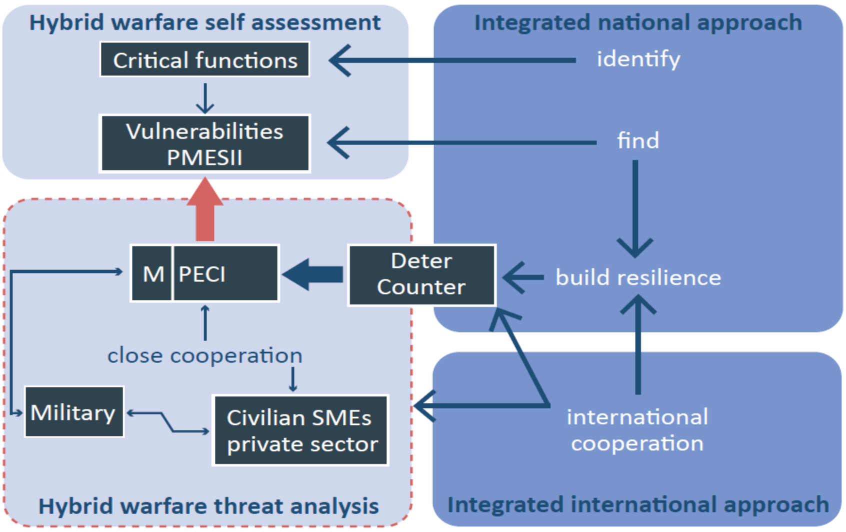
Hybrid warfare self assessment
Critical functions
Vulnerabilities PMESII
Integrated national approach
identify
find
M
PECI
Deter Counter
build resilience
close cooperation
Military
Civilian SMEs private sector
international cooperation
Hybrid warfare threat analysis
Integrated international approach

Figure 2: MCDC theoretical model – understanding HW and identifying specific strategies
Source: Multinational Capability Development Campaign (MCDC). Understanding Hybrid Warfare. January 2017. Figure 5; p. 23. Available from https://bit.ly/3jwwoJI

Practically, using data from figure 2, first of all, it is important to conduct a HW threat analysis based on the smooth cooperation between military and civilian subject matter experts (SMEs) to cover all domains from MPECI. Next, the HW threat analysis is used to perform HW national self-assessment to identify PMESII vulnerabilities and critical functions that in turn serve as ingredients for building resilience through an integrated national and international approach. Finally, through the national and international cooperation, the attacker's MPECI is deterred and defeated using tailored strategies. Specific strategies for deterrence are denial deterrence and punishment deterrence. The first strategy, denial deterrence means "*to show the hostile actor that one can easily absorb the attack with minimal costs to the state that is the target of the hybrid activity*" [12], while punishment deterrence is about "*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*" [13]. If deterrence strategies do not generate the desired effects, other response strategies will be used, either defensive (AHW), offensive (CHW), or both. In this regard, defender may use [14]:

- Engage or disengage – correlated to the amplitude of attack and the necessity of reacting;
- Inward or outward – the response could be directed either on defender's capabilities or on attacker's capabilities;
- Overt or covert – the response could be public and official or undercovered with a limited audience;
- Coerce or induce – the response could be assertive or focused on inducing cooperation with the attacker.

All these strategies can be used by defender in any possible combination to generate a tailored response (any combination of offense and defense) to HW manifestations. Also, denial deterrence could be used as a defensive strategy, while punishment deterrence as an offensive one.

4.2. Blue instruments and capabilities

Similar to the attacker, the defender may also use about the same instruments to deny undesired behaviours from attacker's side. More specifically, the defender may use the MPECI tool to engage attacker's PMESII vulnerabilities in order to deny or limit his success. Also, as we have shown previously, when analysing the blue strategies used to escalate vertically and horizontally, another tool that can be used by defender is DIMEL, or in a more comprehensive formula DIMEL plus finance and intelligence (DIMEFIL). All these tools, as well as other existing tools, are somewhat similar because they are used for the same purpose. However, there are some differences given by the inclusion or exclusion of some reference domains. Concerning about the capabilities used to react in the HW framework, they cover multi-domains and are engaged through a joint, interagency, intergovernmental and multinational (JIIM) approach.

5. Conclusions

As we have seen, approaching the HW from the behavioural perspective of different opponents is an extremely difficult challenge, because the volatility, uncertainty, complexity and ambiguity (VUCA) of the attackers also spread over the defenders. For this reason, the blue behaviours are always relative and make sense only in relation to the attacker and the conditions existing in the operational environment. Therefore, the most important conclusions that can be drawn from this research are:

- During the HW phasing, the attacker and defender's operational behaviours are either offensive, defensive, or both, with a dynamic of action-reaction-counteraction (red-blue dualism);
- The attacker and defender's behaviours are shaped by specific strategies, instruments and capabilities;
- Red strategies comprise conventional, unconventional, coercion, subversion, proxies, while blue strategies are the CPPCC, resilience, denial deterrence, punishment deterrence, AHW and CHW, with all derived forms; for both opponents, the strategies are not limited to the highlighted ones;
- Either for attacker or for defender, specific power instruments used in HW framework to engage PMESII vulnerabilities are MPECI, DIMEL, DIMEFIL (any other combination of domains is possible);
- In the HW context, regardless of the actor's position (red or blue), the capabilities are multi-domain in fashion and are employed in accordance with a comprehensive approach (JIIM).

Finally, the necessity for identifying the optimum solutions to respond to the HW manifestations requires, primarily, the ability to decipher the opponent's behaviour, which implies the transposition of defender in the mind of the attacker ('to think in red'). In this regard, abilities as preemption and mental agility of multi-level and multi-domain SMEs and decision-makers are required.

Acknowledgements

This paper was written under the research project "*Interdisciplinary Education and Training on Hybrid Warfare*" (KA220-HED-B9458C8A), funded by ERASMUS+ for the time period of 1st November 2021-31st October 2024.

References List

[1] Multinational Capability Development Campaign (MCDC). Countering Hybrid Warfare. March 2019; p. 3. Cited at April 5, 2022. Available from https://bit.ly/3j71kQA.

[2] Ibidem.

[3] Council of the European Union. Food-for-thought paper "Countering Hybrid Threats". Brussels: European External Action Service (EEAS); May 2015; p. 2. Cited at April 5, 2022. Available from https://bit.ly/3DGihuB.

[4] Ibidem, pp. 4-6.

[5] Richterova J. Background Report: NATO Hybrid Threats. Prague: 2015; p. 10. Cited at April 5, 2022. Available from https://bit.ly/3xlDedt.

[6] Cederberg A. Hybrid Warfare. Geneva Center for Security Policy (GCSP): 2015. Cited at April 6, 2022. Available from https://bit.ly/3LJgZ4R.

[7] Council of the European Union. Joint Communication to the European Parliament and the Council - Joint Framework on Countering Hybrid Threats: a European Union Response. Brussels: European Commission; April 2016; p. 2. Cited at April 6, 2022. Available from: https://bit.ly/3DIKscy.

[8] Council of the European Union. Food-for-thought paper "Countering Hybrid Threats". Brussels: European External Action Service (EEAS); May 2015; p. 2. Cited at April 6, 2022. Available from: https://bit.ly/3DGihuB.

[9] Multinational Capability Development Campaign (MCDC). Countering Hybrid Warfare. March 2019; p. 13. Cited at April 6, 2022. Available from https://bit.ly/3j71kQA.

[10] Cîrdei A. Countering the Hybrid Threats. Land Forces Academy Review. 2016. No 2 (82): p. 117. Cited at April 7, 2022. Available from: https://bit.ly/3JtT8Vj.

[11] Sweijs T., Zilincik S., Bekkers F., Meessen R. A Framework for Cross-Domain Strategies Against Hybrid Threats. Den Haag: Hague Centre for Strategic Studies (HCSS) TNO; 2021; p. 4. Cited at April 9, 2022. Available from: https://bit.ly/3reuHVJ.

[12] Kersanskas V. Deterrence: Proposing a more strategic approach to countering hybrid threats. Helsinki: European Centre of Excellence for Countering Hybrid Threats; March 2020; p. 11. Cited at April 9, 2022. Available from: https://bit.ly/3E2oYr4.

[13] Ibidem, p. 12.

[14] Multinational Capability Development Campaign (MCDC). Countering Hybrid Warfare. March 2019; pp. 53-54. Cited at April 9, 2022. Available from: https://bit.ly/3j71kQA.