INTRODUCTION – HYBRID WARFARE AND GREY ZONE

Nowadays, the way state and non-state actors promote their security interests has evolved with the same speed as the technical evolution and military thinking. This is the reason why practitioners and academics all over the world debate concepts like hybrid warfare (Hoffman, 2007, p. 8) or grey zone conflict (Mazarr, 2015, p. 101) while referring to the modern warfare. Both concepts are interconnected because modern hybrid warfare primarily occurs in the grey zone (Dowse, Bachmann, 2021), where state and non-state actors apply unconventional tools and hybrid techniques (Carment, Belo, 2021). Moreover, the use of non-state entities does not cross over the limit into classical state-level aggression (Belo, Carment, 2021). In this case, the aggressed actor is not able to react due to the ambiguity of international law, of the aggressor’s actions and the impossibility of attack attribution (Bachmann, Dowse, 2019).

The concept of hybrid warfare was proposed in the early 2000s by Frank Hoffman as being a theory of military strategy, which implies political warfare and blends simultaneously lethal and non-lethal actions using conventional weapons, irregular tactics, terrorism, cyberwarfare, as well as other influencing methods, such as fake news diplomacy, lawfare and foreign electoral intervention (Reid, 2018) with the aim to disrupt and disable an opponent’s actions without engaging in open hostilities (Bachmann, Dowse, 2019).

It is not enough to mix regular with irregular elements, kinetic with non-kinetic, to achieve the hybrid character, but the positioning of the event in the grey area (Meyers, 2016, p. 14) is more effective. This is the reason why other authors emphasize more the fact that the aggressor state actors do not want to assume responsibility for the actions they undertake and carry out activities in fields not regulated by international law. So, they consider the concept of grey-zone conflicts...
or warfare being sometimes different from the concept of hybrid warfare (Stoker, Whiteside, 2020, pp. 1-37). Conducting operations in the “grey zone” of conflict means that operations may not clearly cross the threshold of war. In this situation, the new type of war produces dilemmas regarding the legal issues, as the states have established clearly the aspects that are allowed during peacetime or during war. But with the exploitation of hybrid methods of some vulnerabilities in order to achieve desired but not acknowledged effects by bringing the conflict into the grey zone, the situation requires a new approach based on a legislative point of view (Mazarr, 2015, p. 108). Democratic states need new tools to respond to grey-zone threats because their legal systems are oriented towards approaching conflicts through the lens of war and peace with very little preparation for anything in the grey zone (Belo, Carment).

Grey zone tactics are often used by weaker state actors who enforce them against inferior democratic state actors to advance their regional interests (Mazarr, p. 120). Due to the lack of situational awareness, this can lead democratic states to either dramatically overreact or underreact when faced with grey-zone challenges (Belo, Carment, 2021).

As stated previously, hybrid warfare has been defined as a combination of means like symmetrical and asymmetrical (Mansoor, 2012, p. 3), regular and irregular, conventional and unconventional to bewilder the adversary (Andersson, Tardy, 2015). But if we analyse the historical examples such as the Trojan horse and the examples from Sun Tzu’s Art of War, we can observe that this type of war has been practiced since ancient times if we were to describe the proximate genre of the definition just by associating the above terms (Meyers, 2016, p. 17). But the major difference between those historical examples and today’s warfare is that in the past irregular tactics were used by less powerful state actors out of the need to defend themselves in a declared war situation. Nowadays, these tactics are used by powerful regional state actors because they have proven to be very effective (Thiele, 2015, p. 56), they are carried out in the legally unregulated grey area and frequently before or even without starting a war.

“We must keep in mind that <hybrid> refers to the means, not to the principles, goals, or nature of war” (Schadlow, 2015), but positioning the event in grey area highlights its volatile, uncertain, complex and ambiguous (VUCA) character (Kraaijenbrink, 2018), by exploiting an unregulated environment from the international law perspective. In the next section, we will analyse the means of the hybrid warfare with the purpose of creating a new analytical tool by using the Black Sea Snake Island hypothetical case study.

**SNAKE ISLAND**

Snake Island, or Ostriv Zmiinyi in Ukrainian and Insula Șerpilor in Romanian is a Ukrainian islet of 17 hectares situated in the proximity of the Danube Delta in the Black Sea, which was the subject of delimiting the continental shelf and the exclusive economic zones appertaining to Romania and Ukraine in the Black Sea at the International Court of Justice between 2004-2009 (ICJ Reports, 2009).

According to the rules of international law, both states requested to the International Court of Justice to draw a delimitation line, defined by geographical coordinates, as shown in figure no.1.
The International Court of Justice deliberated in 2009 that the Snake Island was too far from the seashore and too small to represent a point which could contribute in setting boundaries and it placed 9,700 square kilometres of waters under Romania’s control, as seen in the figure no 1. This decision and the new development of the Black Sea gas fields offer the premises to make Romania one of the biggest European Union’s natural gas producers (Emerging Europe Staff, 2022) and a rival for Russia in the regional natural gas market (Harm, 2022).

WHAT IF SNAKE ISLAND WILL BE UNDER THE CONTROL OF A STATE ACTOR WITH AGGRESSIVE BEHAVIOUR?
Taking into consideration that the islet represented for Russia an objective starting on the first day of the Ukraine invasion when it was occupied by the aggressor, we can deduce that Snake Island has a major significance related to military and energy security. As a consequence, the island still presents great interest for Russia and serves some goals, as follows (ib.):

• to seize key maritime terrain to control sea lines of communications (SLOCs) between Odessa and Bosphorus;
• to establish offensive capabilities in order to monitor NATO activities;
• to contest the decision of International Court of Justice in order to claim parts of offshore gas platforms like the XIII Pelican, EX-27 Muridava, and EX-28 EST Cobălcescu concessions located in NATO member Romania’s Exclusive Economic Zone (EEZ) as seen in figure no. 2.

By using military, political, economic, civilian and informational (MPECI) instruments of power, a potential aggressor can exploit Romania’s vulnerabilities in order to produce effects in the energy infrastructure domain. We will analyse this topic by proposing a seven-step algorithm to identify hybrid warfare with three purposes: to visualize the hybrid warfare (Steps 1-4), to test the means used by an aggressor by using Process Tracing in order to establish if these are necessary and sufficient for the aggressor to produce desired effect(s) (Step 5),

1. Research Methods
This paper is based on Patrick J. Cullen and Erik Reichborn-Kjennerud Analytical Framework model for visualizing the hybrid warfare (Cullen, Reichborn-Kjennerud, 2017, pp. 16-25) applied to the particular Snake Island situation in order to identify critical functions and vulnerabilities, synchronization of means and actions and desired effects of the hybrid warfare actor. Moreover, we have applied Process Tracing to identify vulnerabilities in order to establish which of them can create the most disastrous consequences for Romania’s energy security. Finally, we will use a Measure of Performance (MOP) tool in order to evaluate the aggressor means progress in obtaining his desired effect(s).
and to apply MOP tool in order to evaluate the aggressor’s operation progress (Step 7). Moreover, during the algorithm, we have inserted a redundancy measure (Step 6) for reassessing the aggressor desired effect(s) as presented below.

2. Results and Discussions

Steps 1-4 - Analytical Framework model

The Analytical Framework model has been developed by the above-mentioned authors to help the readers understand the nature of hybrid warfare (ib., p. 16) and it focuses on the aggressor’s use of the MPECI (military, political, economic, civilian and informational) instruments of power against the aggressed state actor’s PMESII (political, military, economic, social, information and infrastructure) sectors in three phases: normality, crisis and emergency, as presented in figure no. 3.

Overview

An aggressor state actor takes actions to prevent Romania from extracting offshore gas resources from its exclusive economic zone. This case study highlights a situation of a state actor’s use of synchronized military and political levers to demonstrate a hybrid approach to achieve an infrastructure effect.

Vulnerabilities:

| V1 | Romania’s limited military naval capabilities to protect its exclusive economic zone (EEZ). |
| V2 | The limitations imposed by the Montreux Convention to request NATO military capabilities in order to protect Romania’s EEZ. |

Means:

| M1 | Contest the decision of the International Court of Justice in order to claim parts of offshore gas platforms like the XIII Pelican, EX-27 Muridava, and EX-28 EST Cobălcescu concessions located in NATO member Romania’s Exclusive Economic Zone (EEZ). |
| M2 | Prevent Romania from exploiting its resources by using maritime blockades in the EEZ and unassumed drone attacks to energy critical infrastructure. |

Effects:

| E1 | Romania’s impossibility to extract energy resources from its EEZ. |

In our case study, in Step 1, in an ordinary situation, we can identify two vulnerabilities related to Romania’s offshore gas extraction, which constitute enabling factors for a potential aggressor to use a hybrid synchronized attack package – SAP (Cullen et al., p. 16):

- Vulnerability V1 related to Romania’s actions/inactions;
- Vulnerability V2 related to the Montreux Convention.

In Step 2, we correlate the identified vulnerabilities with PMESII domains for understanding where they take place and which are the domains where the aggressive actor may apply the hybrid synchronized package.

Moving on to Step 3, based on situational awareness and early warning indicators, we could identify the means used by the aggressor to exploit identified vulnerabilities. Usually, these levers are difficult to discover in the early period of a hybrid attack, as the first of them are meant to shape the environment to bolster the main effort.
Finally, in Step 4 of the Analytical Framework model, we estimate the aggressor’s desired effect(s) related to the identified vulnerabilities from Steps 1 and 2 and the means used during Step 3.

Step 5 – Testing the means used by an aggressor in order to establish if they are necessary and sufficient to produce their desired effect(s)

During this step, we expand the analysis of how we should judge competing explanatory claims (Bennett, 2010) by using a fundamental method of qualitative analysis named Process Tracing. This mode of analysis provides consistency to our algorithm by drawing descriptive and causal inferences from particular evidence, sometimes analysing the sense as part of a temporal sequence of events or phenomena (Collier, 2011, p. 843). Process Tracing research probes the theoretical causal mechanisms linking causes and outcomes together (Beach, 2017, p. 2), being similar to a method used by detectives to solve a crime by analysing the clues and identifying possible perpetrators by using questions (Bennett).

By using this method, our objective is to test the means in order to establish if they are necessary and sufficient to generate the aggressor’s desired effect(s).

As it is presented in table no. 1, two vulnerabilities V1 and V2 combined with means M1, necessary but not sufficient, cannot produce the effect E1 in the infrastructure domain. In this situation, this type of grey zone action fails because M1 is only necessary but not sufficient for triggering an emergency effect like E1. By only contesting the decision of the International Court of Justice, we expect that the state actor with aggressive behaviour intends to shape the environment for the moment when M2 produces effects. This is the reason why at this time, when only M1 takes place and not M2, it is very difficult to estimate what the real effect that aggressor state actor wants to achieve.

<table>
<thead>
<tr>
<th>Necessary to produce the aggressor desired Effect/s</th>
<th>Sufficient to produce the aggressor desired Effect/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>1. Straw in the wind</td>
<td>3. Smoking gun</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>2. Hoop</td>
<td>4. Doubly decisive</td>
</tr>
<tr>
<td>M1*</td>
<td></td>
</tr>
</tbody>
</table>

Table no. 1: Process Tracing method to identify means (M1) to confirm causal inference

*M1 – Contest the decision of the International Court of Justice in order to claim parts of offshore gas platforms like the XIII Pelican, EX-27 Muridava, and EX-28 EST Cobălcescu concessions located in NATO member Romania’s Exclusive Economic Zone (EEZ)

Going further, if M2 takes place at the same time as M1, it will change the situation drastically. In the case when an aggressor state actor carries out a maritime blockade and other hybrid tactics in Romania’s exclusive economic zone (EEZ), Romania cannot extract the energy resources from the territory that the International Court of Justice attributed in 2009 because of an additional means M2 which is necessary and sufficient to create a strong effect like E1 presented in table no. 2. In this situation, the type of hybrid actions are CONFIRMED. In other situations, we cannot preclude the possibility that 2, 3 or more necessary but not sufficient means can be well synchronized to produce an effect like E1.

<table>
<thead>
<tr>
<th>Necessary to produce the aggressor desired Effect/s</th>
<th>Sufficient to produce the aggressor desired Effect/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>1. Straw in the wind</td>
<td>3. Smoking gun</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>2. Hoop</td>
<td>4. Doubly decisive</td>
</tr>
<tr>
<td>M1</td>
<td>M2**</td>
</tr>
</tbody>
</table>

Table no. 2: Process Tracing method to identified means (M2) to confirm causal inference

**M2 – Preventing Romania from exploiting its resources by using maritime blockades in the EEZ and unassumed drone attacks to critical energy infrastructure
Step 6 – Reassess the aggressor desired effect(s)

This stage of our analysis represents one of the most difficult parts, because it is based only on estimations. The role of these estimations is not to predict what the enemy will do next, because it is almost impossible, their role is to diminish uncertainty (Harm, 2022). This is the reason why in our analysis we reassess the estimation regarding aggressor desired effect(s) during Step 6, by taking into consideration the evaluations from steps 1-5. If the aggressor’s desired effect(s) is/are confirmed, we should go on the last step, if not, we should reanalyse the means or try to find more cues.

Step 7: Test all means by using MOP tool in order to evaluate the aggressor’s operation progress

In the last step, we should apply the second test to all the identified means by using a military evaluation tool Measures of Performance (MOP). Usually, this tool is analysed in conjunction with Measures of Effectiveness (MOE) which represent an indicator that helps to answer the question “Are we doing the right things?”. This tool is used to measure changes in system behaviour, achievement of an objective or contribution to the creation of an effect by comparing multiple observations over time (Wade, 2016, pp. 1-70; 2020, pp. 1-67).

Measure of Performance (MOP) is an indicator which helps to answer the question “Are we doing things right?”. This tool is used to assess action that is tied to measuring task accomplishment and confirms or denies that a task has been properly performed (ib.).

Both tools are usually used to assess and evaluate the operation for friendly forces in order to determine if they are doing the right thing in the right way.

In our case, in the seven-step algorithm to identify hybrid warfare, we select only the MOP tool in order to measure the aggressor’s means progress in achieving the desired effect(s). So, the question “Are we doing things right?” will become “Are they doing things right?”. Moreover, we take into consideration quantitative (observation-based) indicators and qualitative (opinion-based) indicators to determine the desired conditions (DC) that the aggressor wants to achieve, desired Effect(s), as presented in tables no. 3 and no. 4. Below are estimated only few of the aggressor’s desired conditions for implementing M1 and M2. These desired conditions presented in tables no. 3 and no. 4 and in figure no. 4 are fictitious and have been brought up only to explain the method of analysis.

### Table no. 3: Desired conditions for implementing M1

<table>
<thead>
<tr>
<th>No</th>
<th>Desired conditions (DC)</th>
<th>Counting desired conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC 001</td>
<td>Percent/number of press articles that support the aggressor claims</td>
<td>NO 20% YES 80%</td>
</tr>
<tr>
<td>DC 002</td>
<td>Percent/number of Non-Governmental Organization (NGOs) that support the idea that oil extraction in the EEZ affects the flora and fauna of the Black Sea</td>
<td>NO 60% YES 40%</td>
</tr>
</tbody>
</table>

### Table no. 4: Desired conditions for implementing M2

<table>
<thead>
<tr>
<th>No</th>
<th>Desired conditions (DC)</th>
<th>Counting desired conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC 004</td>
<td>Percent/number of unassumed anti-ship mines in the perimeter of the extractions</td>
<td>NO 30% YES 70%</td>
</tr>
<tr>
<td>DC 005</td>
<td>Percent/number of unassumed Unmanned Surface Vehicles (USVS) and Unmanned Aerial Vehicle (UAV) in order to disrupt the extraction in Romania EEZ</td>
<td>NO 25% YES 75%</td>
</tr>
<tr>
<td>DC 006</td>
<td>Percent/number of days/year of marine blockades in the Romania EEZ</td>
<td>NO 60% YES 40%</td>
</tr>
</tbody>
</table>

Evaluation includes considering whether the desired conditions have changed or are still achievable through the current hybrid aggressor operational approach. At this level, it is important that the desired conditions are measurable in order to determine the aggressor’s progress in numbers or percentage as seen in figure no. 4. This step can be developed by simply collecting open source
information from media and social media, but it may be more efficient if specific intelligence collecting tools are used.

During this seven-step algorithm fully presented in figure no. 5, analysts and staff permanently challenge the key assumptions made when framing the problem. In the situation when a hypothesis is not validated, then reframing is the solution.

**Step 1:** Identify own vulnerabilities.

**Step 2:** Establish PMESII domains for own vulnerabilities.

**Step 3:** Identify means used by the aggressor to exploit identified vulnerabilities.

**Step 4:** Estimate the aggressor’s desired effect(s) related to vulnerabilities and means.

**Step 5:** Test the means by using Process Tracing method in order to establish if these are necessary and sufficient to produce the aggressor’s desired effect(s). If not, find more means until they, analysed individually or collectively, are both necessary and sufficient.

**Step 6:** Reassess the aggressor’s desired effect(s).

**Step 7:** Test all means by using MOP tool in order to evaluate the aggressor’s operation progress.
CONCLUSIONS

In conclusion, we have combined three research methods and tools: Analytical Framework model for visualizing hybrid warfare, Process Tracing to confirm or infirm the tools used by the aggressor and a military tool, Measure of Performance, to evaluate the aggressor’s progress in a Black Sea Snake Island hypothetical case study. These 3 research methods and tools are structured in a seven-step algorithm to identify hybrid warfare, as detailed in figure no. 5, with the purpose of creating an algorithm to identify and evaluate hybrid warfare. All three methods are important because the Analytical Framework model for visualizing hybrid warfare (steps 1-4 and 6) helps practitioners to perceive their own vulnerabilities, the aggressor’s means and desired effect(s), Process Tracing (step 5) to test the means in order to establish if they are necessary and sufficient to produce the aggressor’s desired effect(s) and the last tool, Measure of Performance, (step 7) in order to evaluate the aggressor’s operation progress.

This algorithm, like any other analytical tool, has some limitations and they are imposed by the complexity of the war and by the principle action-reaction-counterreaction, which creates the conditions for permanent assessment and adaption. Secondly, this algorithm is based on estimations and the results may be affected by the analysts’ perceptions or experience. Thirdly, this algorithm offers only the possibility to visualize, to confirm or infirm an aggressor’s actions and to evaluate their progress without creating the instruments for countering their hybrid actions. Even though the seven-step algorithm to identify hybrid warfare is limited, this tool may represent a starting point for other hybrid warfare analyses meant to understand hybrid warfare as more than a simple combination between lethal and non-lethal actions using conventional weapons, irregular tactics, terrorism, criminal behaviour and cyber warfare.

By applying the algorithm in the Black Sea Snake Island case study, we can conclude that for a democratic state actor like Romania, NATO and EU member state, to counter this type of hypothetical scenario, it is important to invest and to develop more the naval and air military capabilities for mitigating vulnerabilities and increasing energy security in the Black Sea region. As presented in the Analytical Framework model for visualizing hybrid warfare, PMESII domains are interconnected and vulnerabilities in the military or political domain exploited by an aggressive behaviour state actor with a synchronized attack package with necessary and sufficient means can contest the existing rule-based regional order and can create disastrous effects in energy and infrastructure domains transforming the 17-ha Snake Island into one of the biggest game changers in European energy security.

BIBLIOGRAPHICAL REFERENCES:


