Identifying Factors to Compare Responses to Hybrid Threats: Analysis of Strategic Cultures to Understand Country Differences

Bas Keijser and Kimberley Kruijver
TNO Defence, Safety & Security
The Hague
THE NETHERLANDS

Bas.Keijser@tno.nl & Kimberley.Kruijver@tno.nl

ABSTRACT

The changing security environment the Alliance faces today includes the emerging threat of hybrid conflict. This influences NATO's deterrence and defence posture. Examples include: information manipulation and interference by foreign actors, targeted actions aimed at disrupting infrastructure or proxy activities paving the way for open war. Various member states have institutionalised counterhybrid strategies, legislations, decision-making processes and tailored policy measures to respond to such threats. These instruments can have a positive effect on the resilience of a society and a deterrent effect on adversaries. To investigate different national responses, they need to be placed in a country's specific context in terms of basic geographical, historical and social characteristics as well as its strategic culture. Strategic culture refers to norms, ideas and practices that influence decision-making and ultimately the creation of a grand strategy to achieve strategic political objectives. Whereas strategic culture analysis is traditionally focused on explaining the use of force in international relations, we hypothesise that there is merit in applying it to a broader range of responses at a state's disposal, specifically in the context of hybrid threats. Analysing strategic cultures this way may enhance understanding of various member states' responses to hybrid threats and thus contributes to understanding of NATO's deterrence and defence posture.

Keywords: Hybrid threats, Strategic culture, Hybrid response, Hybrid defence and deterrence

1.0 INTRODUCTION

The security environment has changed rapidly, which is reflected in the numerous shapes and forms of threats to national security nations have to deal with [1]. An important part of this is the threat of hybrid conflict, defined here as "a conflict between states that falls largely below the threshold of open armed conflict, and involves the integrated use of means and actors, in pursuit of certain strategic objectives" [2]. Hybrid conflict can take shape in the form of hybrid interference, disruption and warfare ([3], p. 11). Specific demographic or socio-economic groups are influenced to induce societal tensions. Opaque investment from ultimately state actors creates strategic dependencies in vitally important sectors of the economy. Targeted actions may aim at disrupting infrastructure. And proxy activities by militarised groups threatening the security in border regions are used to destabilise or pave the way for open war.

Societal resilience is important to counter such hybrid threats. This refers to "the ability of states and societies to deter, resist and overcome the impact of external interference" by state actors ([4], p. 26). Thus, resilience makes a country as a whole more resistant to influencing and attacks. Governments and civil society can reduce vulnerabilities to hybrid exploitation by reducing dependencies and preparing for hybrid activities through exercising what-if situations [3] Complementarily, various member states have designed and implemented counterhybrid strategies, drafted legislations, adopted decision-making processes and tailored policy measures to respond to such threats. These are frequently part of a broader framework of national security or defence policy. Because the contextual situation of every NATO member state differs, the exact motivation and strategic choices to increase resilience and respond to hybrid threats also differ. For example, countries on Europe’s Eastern flank perceive other hybrid threats than countries in North America, and thus decide to take other resilience and response measures. Some countries have a history of mitigating national security threats through government intervention, whereas in other countries civil society also has an important role in defence.

To understand NATO’s deterrence and defence against hybrid threats it is important to understand what individual nations do to cope, since the primary responsibility of countering hybrid threats[1] lies with the targeted country [5]. In the end, the sum of national resilience and response to hybrid threats forms the foundation of NATO’s deterrence and defence posture against hybrid threats, together with complementary coalition efforts. Furthermore, to comprehend the responses to hybrid threats, it is beneficial to investigate underlying reasons for differing responses. Thus, the central question of this research is: **What factors can be identified to explain differences between how countries counter hybrid threats?**

In this paper we use the concept of strategic culture[2] as a framework to answer the research question. As opposed to the traditional use of strategic culture to explain the use of military force, we re-apply the concept of strategic culture to countering of hybrid threats. Based on literature on strategic culture and hybrid response, this paper develops a conceptual framework, which is recommended to be applied in follow-up research. Our contribution to practice thus is twofold: this conceptual framework of explanatory factors can support comparing hybrid response across countries and can contribute to better cooperation between countries.

2.0 BASICS OF COUNTERING HYBRID THREATS

To investigate the various strategies that states take to counter hybrid threats, it is first important to explain how counterhybrid measures are taken. These measures are taken on the basis of situational awareness of a hybrid threat [6], [7]. Given a specific hybrid threat, e.g. a possible cyberattack on a critical information system, various counterhybrid measures can be taken at various points in time, before, during or after a hybrid activity. When a counterhybrid measure is taken before an activity, we speak of a threat reduction measure. When hybrid threats eventually materialise, we say that a hybrid activity takes place. The EU Joint Framework in this regard already spoke of “preventing, responding to and recovering from” hybrid activities [8].

In the following discussion, we have placed the counterhybrid measures on a timeline. Even though it is difficult to categorise hybrid activities this way, it can help the discussion about various measures at a country’s disposal. For example, before a disinformation campaign aiming for influence within a specific social group takes place, different measures can be taken: disrupting cyber influencing capabilities of an actor, strengthening disinformation awareness within the social group, and identifying and supporting vulnerable members of the social group to later counter the disinformation narrative. In the time frame of the disinformation campaign itself various measures can also be taken: e.g. try to expose platforms, channels and accounts of disinformation while the campaign takes place, or investigating the disinformation campaign to be better able to reduce adverse effects of the narrative. After the disinformation campaign has taken place, the uptake of the disinformation narrative can be investigated to actively counter with a truthful narrative.

From the examples above it is apparent that the eventual effect of a measure does not always happen before the threat materialises, i.e. the disinformation campaign takes place. In some cases, the goal of a measure is to have effect only during or after threat materialisation. Of course, the actual effectiveness of the disinformation campaign in the example is dependent on many things including the ability to identify the

[1] In ‘countering hybrid threats’ we include both preventive measures aiming at resilience, as well as reactive measures taken to respond after a hybrid activity takes place. See also the elaborations in later sections.

[2] We use the concept of strategic culture as it is understood in international relations or strategic studies literature [11], [12]. In many other literatures organisational culture, political culture or more generally national culture are studied. These concepts might also shed light on how hybrid threats are perceived and responded to, but are not the focus here.

quality of information in the wider population. Thus, broad education measures are also important to create awareness and identify disinformation unrelated to a specific campaign. Combining these two axes, when a measure is taken and when its effect materialises, a categorisation of measures is construed (see Table 1).

Table 1: Categorisation of measures related to an illustrative hybrid activity, for the example of a disinformation campaign aiming for social influence.

	Measure Before Activity	**Measure During Activity**	**Measure After Activity**
Effect before activity	Disrupt cyber influencing capability	*Not possible*	*Not possible*
Effect during activity	Strengthen disinformation awareness in social group	Expose disinformation presence on platforms used	*Not possible*
Effect after activity	Identify and support people vulnerable to disinformation	Investigate disinformation narrative	Investigate disinformation uptake, design counternarrative

A number of concepts are frequently used to characterise counterhybrid measures. Firstly, **measures taken can have a resilience effect**. Measures that contribute to resilience to a specific hybrid threat can be placed in the first column of Table 1. However, the effect of the increased ability of states and societies to overcome the impact of a hybrid threat can either take place before, during or after a hybrid activity takes place. States and societies are either less vulnerable, better defended, or more adaptive at recovery.

Secondly, **measures taken can have a deterrence effect** – i.e. the measures have an influence on the decision calculus of the hybrid actor posing the threat [9]. Measures taken to deter an actor from a specific activity should also be in the first column of Table 1, for their objective is to prevent a threat to materialise, thus they will initially be taken before an attack occurs. Deterrence-by-denial is aimed at denying the hybrid actor its perceived benefits. This can for instance be done by increasing the resilience of a society against a specific type of hybrid activity. Thus, some measures can both have a resilience effect as well as a deterrence effect ([9], p. 13). While deterrence-by-punishment threatens a hybrid actor with costs if an activity is performed, these are imposed after the fact, and thus the actual punishment is seen in the lower-right cell of Table 1.

Thirdly, **measures can also be taken as a response to a hybrid activity** ([6], p. 51), which should be placed in the second and third column of Table 1. The goal of responding to hybrid activities that take place is to "disrupt or prevent an adversary from taking further hybrid aggression" ([6], p. 60). They thus acknowledge that the goal is to both discontinue hybrid aggression as well as to deter further aggression in the future. Measures taken as a response can apply all DIMEFIL[3]-instruments of power, varying from expelling diplomats, to instating economic sanctions or voicing military threats.

It is important to emphasize that the framework above cannot reflect the full complexity of hybrid threats and corresponding countermeasures. First, since multiple threats can occur in parallel or after each other, response measures can have a preventive effect on a future similar activity ([9], p. 7). I.e. imposing sanctions as retaliation aims to deter further cyberattacks. Furthermore, one measure can be aimed at reducing multiple threats concurrently. An example of this are broad legislative changes, i.e., cybersecurity legislation at the EU-level setting common standards for infrastructure protection ([10], p. 1086). Third, time scales of threats and activities are frequently drawn out over longer periods of time. Strategic dependencies take years or even

[3] Framework describing elements of power: diplomatic, information, military, economic, financial, intelligence, law enforcement.

decades to take shape. At the same time, countermeasures aimed at e.g. reduction of vulnerability can also take a long time. Finally, because of the often limited available information, analysts and decisionmakers can be unaware that a hybrid activity has already started. This means that those activities can still have their long term effects at a later point in time.

3.0 BASICS OF STRATEGIC CULTURE

Strategic culture is a concept that originated to explain strategic decision-making with regards to security and the military on a national level [11], [12]. Since its conception, the term has been interpreted and applied in different ways. A key point of discussion centres around the question whether strategic culture determines (Johnston) [12] or merely shapes decision-making (Gray) [11]. However, the use of military force and the decision-making processes leading to employing such force have remained key aspects of its understanding. This paper adheres to the conceptualisation of Biava, Drent & Herd [13] and thereby follows Gray's line of thinking in that strategic culture revolves around norms, ideas and practices that *shape* decision-making processes and eventually a grand strategy to accomplish strategic political objectives. Thus, to properly understand the strategic culture of a country the authors argue that a researcher should ask "when, where, how and why [a state] uses a range of appropriate instruments […] to achieve strategic political objectives" ([13], p. 1234). It is important to emphasise that (perceptions of) external factors, such as geography or crises, also influence strategic decision-making. This operationalisation already widens the scope of the relevance of strategic culture from a focus on the use of military force to include all DIMEFIL-instruments of power, thereby making it applicable to the context of hybrid threats.

Effectively, the concept of strategic culture can be used to argue that the intrinsic and unique characteristics of each nation are reflected in their decision-making processes [14]. Therefore, the key aspects of the concept will be used to build a new theoretical framework, with which national responses to hybrid threats can be compared. Whereas the original concept revolves around the use of military force – the political-strategic goals, the doctrinal plans and the actual execution of force [15] – in the contemporary hybrid threat environment much broader activity than traditional kinetic warfighting is used. The original understanding of strategic culture is therefore insufficient to understand the full scope of the current and future national strategic behaviour of countries. Wijnja [16] compared the counterhybrid approaches of Finland, Germany and the Netherlands, applying the original concept of strategic culture to explain the context shaping their approaches. She uses an abstract framework of organisation of security and looks at the country's approaches to detecting, deterring and responding to hybrid threats [6]. While recognising that the organisation of security and specific measures taken to detect, deter and respond differ per country, Wijnja's [16] conclusion is that their general approaches are similar and that therefore differences in strategic culture have a limited influence.

However, the counterhybrid efforts NATO members take are less similar than Wijnja [16] finds. This conclusion can only be drawn after more detailed analysis of counterhybrid responses. Moreover, Wijnja [16] used the original, and thus incomplete, understanding of strategic culture. Given the contemporary application of instruments of state power in hybrid conflict, strategic culture should be extended beyond the Cold War concept ([13], p. 1229). This paper prepares a challenge to Wijnja's [16] observation, by building on the author's own recommendation: to broaden the concept of strategic culture to incorporate hybrid security issues and all the DIMEFIL-instruments. The application of strategic culture to the contemporary and future security environment results in a conceptual framework that can be used to structurally analyse and compare how countries counter hybrid threats in more detail.

Due to the complexity of 'culture' as a whole, it is more feasible to explore distinct factors of strategic culture that are reflected in the relevant aspects of decision-making related to counterhybrid efforts [17]. A suitable dynamic conceptualisation of strategic culture emphasises the constant interplay between discourse on the one hand and practice on the other [18]. Thus, in order to reconceptualise the notion, the focus should be directed towards both elicited strategic goals as part of grand strategy *(discourse)* and actual behaviour of the state with regards to hybrid threats *(practice)*. Based on earlier research [19], this leads to the following delineation of the concept on three levels:

1) **The political-strategic level of strategic culture**, which is reflected in the grand strategy of a country, stating a country's hybrid threat perceptions, it's overarching motivations and goals to build resilience and to counter hybrid threats. National decision-making models and processes which underly the hybrid threat strategy should also be taken into account at this level.
2) **The organisational level of strategic culture**, which is reflected in the procedures, organisations and collaborations between these organisations stood up with the aim to build resilience and counter hybrid threats. The designed governance follows from the goals described at the political-strategic level, and naturally also guides the relevant institutions of a country in their behaviour.
3) **The behavioural level of strategic culture**, encompassing the actual counterhybrid practice of a country. How has it built resilience and responded to hybrid threats? How have procedures been used, and what activities have organisations performed alone and in collaboration? What counterhybrid measures were used?

All levels of strategic culture are interrelated and reflect the current norms, values, perceptions and other ideas that are important to a country and thus inform its strategic goals and actual behaviour. The political-strategic level shapes the organisational level, which in turn influences the behavioural level. However, changes in behaviour could have a bottom-up effect in changing policies and governance, which in turn influences grand strategy [19].

4.0 INSTITUTIONALISATION OF HYBRID RESPONSE

Countering hybrid threats is of course much more than just taking individual measures with a resilience effect, a deterrence effect, or as a response (see section 2). When a country identifies the need to counter hybrid threats and identifies to-be-implemented measures, it needs to do this sustainably to be most effective. Institutionalisation refers to the sustainable incorporation of counterhybrid activities into an explicit strategy and underlying practical implementations – this shows the interplay between *discourse* and *practice*. Institutionalisation can be done by for example appointing relevant governmental or non-governmental organisations to deal with certain measures to be taken to counter hybrid threats or by creating entirely new organisations or procedures for these tasks. Such NGOs could include existing ones that are providing (preventive) education on how to recognize (online) disinformation or crisis response organisations (responsive) that can be specialised in certain forms of 'hybrid disaster relief'. This could encompass aid when e.g. your internet connection is not working anymore, and you do not have access to fundamentals like your banking account or even your own home. Institutionalising counterhybrid efforts allows for repetitive use of counterhybrid measures[4], evaluating deterrence effects over time, explication of roles and specialisation on the part of responsible agencies.

The process of institutionalisation always takes place in a broader context of a state's geographical and societal background as well as its strategic culture, consisting of threat perceptions, motivations, historical practices and national security decision-making models. These factors are influenced by underlying, existing norms, values, perceptions and other ideas that are prominent in a country. In turn, the other way around: narratives about historical practices also cause societal norms, beliefs and threat perceptions to emerge [20]. Institutionalisation takes place at all three levels of strategic culture: at the political-strategic level new strategies are formalised, at the organisational level agencies are tasked with new roles and at the behavioural level measures are repetitively employed. In general, it can be argued that the political-strategic level represents the factors that influence and thus can explain the institutionalised counterhybrid aspects at the

[4] See also the discussion of the intricacies of the timelines associated with hybrid threats in the last part of section 2, to comprehend why institutionalisation of counterhybrid efforts is necessary.

organisational and behavioural level. On the basis of extensive experience in counterhybrid research, the three levels of strategic culture in Table 2 are operationalised by translating the 'classical' operationalisation of these levels in the strategic culture literature to the hybrid threat environment.

Table 2: Operationalisation of a country's counterhybrid efforts that reflect strategic culture.

At the political-strategic level:	Counterhybrid strategies and legislation
At the organisational level:	Procedures to identify threats, detect, respond and communicate Organisations tasked to perform the procedures above Collaborations between organisations and with other countries
At the behavioural level:	Measures applied to prevent or react to hybrid threats Use of the above procedures Behaviour of organisations with a counterhybrid task Behaviour of collaborations with a counterhybrid task

To structurally analyse and compare a country's so-called grand strategy to counter hybrid threats, a framework of descriptive parameters was construed (see Table 3). This framework builds on the operationalisation of all counterhybrid efforts from the perspective of strategic culture in Table 2, by considering more formal and observable factors (e.g. strategies and legislations, procedures and measures) as well as the underlying informal and less observable factors (e.g. norms, values, perceptions and motivations) that influence decision-making. This is furthermore placed in a country's geographical and societal context.

For example, instead of merely looking at national security strategies, in this framework strategies with specific relevance for (aspects of) countering hybrid threats are looked at. Instead of looking at military doctrines at the organisational level, in this framework counterhybrid procedures are studied. And finally at the behavioural level, actual practices with regards to counterhybrid are taken into account. Because of the inherent complexity of strategic culture as well as institutionalised processes, the descriptive factors are not necessarily disjunct – they often overlap and influence each other. One example is the fact that 'threat perceptions' can be important motivations which can explain certain decisions, but the factor can also be detected quite literally in specific strategy or policy documents.

First the so-called grand strategy of a country needs to be examined (see factors 1 to 5 in Table 3). This starts with a general description of a country's geographical and societal context, which helps to comprehend a country's geo-political situation, it's recent experiences of hybrid activities and inherent societal vulnerabilities. A basic insight into vulnerabilities of a country's security situation can include examples such as the presence of diasporas or extremist political parties, an illiberal media landscape, or a hybrid actor bordering the country – which could form the backdrop of new hybrid threats [21]. Furthermore, the counterhybrid strategy in the broader context of security policy, should be analysed. Describing threat perceptions, motivations and historical practices as well as decision-making models, while taking into regard the underlying norms, values, perceptions and other ideas, makes it possible to place counterhybrid responses in the broader strategic culture [16]. For example, in countries with a long history of territorial integrity issues, threat perceptions also tend to focus on territorial defence (e.g. Poland, see [22]).

Strategy or policy documents are either tailormade for a specific counterhybrid strategy [23] or describe broader security strategies within which hybrid threats are a subject [24]. These strategies serve as high-level guidelines to what a government intends to do to reduce vulnerability and to counter hybrid threats. It is therefore necessary to describe the contours of the strategy or policy and the accompanying legislation [10], as well as the specific topics that are paid attention to, which are indicative of a country's threat perceptions. Some countries have a specific cybersecurity policy to guard against offensive cyber operations directed by state actors, whereas others focus more on threats to economic security, and even other constituting threats including disinformation, election influence, military threats or espionage. Strategy or policy documents can also state the contours of measures to be applied to reduce risk and to respond to activities, as well as which procedures and governance are applied in counterhybrid response.

Table 3: A strategic culture framework of factors to analyse responses to hybrid threats.

Level of Strategic Culture	Factor	Description and Relevant Questions
Counterhybrid grand strategy: broad outline of goals, ways and means. Informed by context, threat perceptions, motivations and decision-making models.	1. Geographical and societal context	Political-strategic: *Basics to understand the country's geopolitical and security situation, and where the threat comes from. What inherent societal vulnerabilities are present? What hybrid activities have taken place in recent years?*
	2. Threat perception of hybrid threats	Political-strategic: *What national security threats are perceived by a country? What is understood as 'hybrid threats'? Is different terminology used to describe (aspects of) 'hybrid'? What underlying values are threatened? What actors are perceived as hybrid threat actors? What is the level of the threat?*
	3. Motivations & historical practices	Political-strategic: *What are the goals for the use of counterhybrid measures? Which norms, values and perceptions underly those goals? What can history tell us about the security and defence practices of a country? Which events have influenced current counterhybrid policies and behaviours?*
	4. Decision-making models	Political-strategic: *How does decision-making on a national level work in general and with regards to security and specifically counterhybrid policy? Which norms, values and perceptions underly national decision-making processes?*
	5. Counterhybrid strategies and legislation	Political-strategic: *What national strategies, policies or high-level guidelines exist that are relevant to hybrid? Which ones are specifically for counterhybrid?*
Counterhybrid procedures: essential steps to react to hybrid threats Informed by grand strategy	6. Procedures for situational awareness, detection, attribution, decision-making, execution and evaluation	Organisational: *What procedures are in place to support the hybrid response cycle consisting of building situational awareness, detection, attribution, decision-making about a response, execution and evaluation?*
		Behavioural: *How have these procedures been used?*
	7. Procedures for risk or vulnerability assessment	Organisational: *What procedures are in place (if any) to perform risk or vulnerability assessment connected to hybrid threats? What is the scope of assessment performed?*
		Behavioural: *How have these procedures been used?*
Counterhybrid governance: tasking and use of procedures	8. Procedures for strategic and crisis communications	Organisational: *What procedures are in place for strategic communications and crisis communications directed at the own population?*
		Behavioural: *How have these procedures been used?*

Level of Strategic Culture	Factor	Description and Relevant Questions
Informed by grand strategy (Cont'd)	9. Organisations and organisational structure with a counterhybrid task	Organisational: *What governmental and non-governmental organisations are tasked with a counterhybrid task? What are their tasks? What tasks are not explicitly given to an organisation?*
		Behavioural: *What activities have these organisations undertaken?*
	10. Collaboration between organisations and with other countries on counterhybrid threats	Organisational: *What collaboration between organisations exists? What collaboration on the topic of counterhybrid efforts does the country have with other countries? What task is given to the collaborations?*
		Behavioural: *What activities have been undertaken in these collaborations? What tasks are not collaborated on?*
Toolbox of measures: performance of tasks	11. Applied measures	Behavioural: *What counterhybrid measures have been applied in practice, across the DIMEFIL-spectrum? What resilience, deterrence effects were reached?*
	12. Prepared measures	Behavioural: *What counterhybrid measures are already actively prepared, but have not yet been used? What are preferences across DIMEFIL-axes? What resilience, deterrence effects are envisioned?*

The grand strategy informs a number of specific procedures to counter hybrid threats (factors 6 to 8). The basic procedure can be seen as a response cycle, consisting of building awareness, detection of threats, decision-making about measures to be taken, execution of measures and evaluation [25], [26],, [6]. In executing measures to prevent or respond to a hybrid activity, there will also be interactions with recovery processes, i.e. when cyberattacks, disinformation campaigns or disruption of vital infrastructure takes place. A further procedure that may or may not be institutionalised and repeated is a risk or vulnerability assessment procedure. Some countries have national security strategies in which repetitive threat assessments or even broader all-hazard risk assessment are performed [27]. In some cases, exercises are also used to identify latent risks or even to practise collaboration in time of hybrid activities ([28], p. 66). Communication procedures, in the sense of strategic communications or crisis communications, towards both the adversary and domestic target audiences can already be designed before a hybrid activity or crisis takes place [29].

In countering hybrid threats existing organisations are provided with new tasks or new organisations are created (factors 9 and 10). To understand organisations that play a part in counterhybrid strategy, their roles, tasks and collaborations need to be described as well as the applicable legal and policy basis. In some cases, the legal and policy basis for performing an individual or collaborative role or task in counterhybrid strategy will already exist, while in other cases new legislation or policy is needed [10]. It is then also important to investigate mandates and accompanying financial and personnel resources available to organisations, this can say a lot about the actual fulfilment of the organisation task in countering hybrid threats. Types of organisations that are likely to be included in countering hybrid threats are: coordination cells, intelligence agencies, research and development organisations, thinktanks, NGOs that support resilience measures, new bureaus in existing policy departments as well as many other executive agencies that have responsibilities to counter specific parts of hybrid threats, e.g. cyberattacks, disinformation campaigns, election influence. For instance, an economic security department or collaborative situational awareness cell might also be stood up to reduce vulnerability to specific hybrid threats.

Because hybrid threats frequently exist across borders, or aim at creating instability within multilateral organisations, collaboration between countries is also very important (factor 10). Legislation and regulation on the multilateral level provides overarching frameworks to protect e.g. economic security and cybersecurity. Within the European Union and NATO, collaboration on the topic of counterhybrid strategy takes place [30], [26], as well as between the two [31]. This also happens in tailored coalitions of like-minded countries.

Moreover, countries apply policy measures to counter hybrid threats (factor 11 and 12). The goal of these measures either is to detect, or reduce risks through resilience and deterrence or to respond to actual hybrid activities. In recent years countries have already taken a large number of measures [32], [33]. Hybrid threats are not new anymore. Thus, counterhybrid measures that were already applied should be described, across societal domains and across instruments of state power on the DIMEFIL-spectrum. Such a detailed analysis can show differences between how countries tend to react to hybrid threats. Some countries have a preference for financial sanctions, while others are more likely to apply military measures. These preferences tend to be informed by for instance threat perceptions and available capabilities. Sometimes a toolbox of measures to be used 'in the event of' is also prepared (e.g. cyber diplomacy, foreign information manipulation and interference and hybrid toolboxes [26], [34]. In some cases, countries signal their readiness to use them to have a deterrent effect on adversaries.

In sum, factors 6 to 12 are the descriptive factors that can be used to characterise institutionalised, organisational and behavioural aspects of a country's counterhybrid efforts. If this exercise is carried out for at least two countries, the results can be compared, and possible differences can come to the fore. However, in order to understand those possible differences better, an analysis needs to be made by taking factors 1 to 5 into account. They namely constitute the possible explanatory elements that also are the key elements of strategic culture, but re-applied to the context of hybrid threats. For example, it can become apparent that country X has counterhybrid processes on the organisational level that are designed around a whole-of-government approach, whereas country Y has similar processes but also involves NGOs and leans more towards a whole-of-society approach. Factors 1 to 5 can then be used to analyse what contributed to these differences. Did the countries experience different historical events that have led them to include NGOs more? Or does one country adhere strongly to the norm that NGOs should function on the same level as their governmental counterparts?

5.0 DISCUSSION

Resulting from the analysis above, two hypotheses for further research can be formed. The first, descriptive, hypothesis is: Countries differ in how they institutionalise their counterhybrid efforts into a counterhybrid strategy, underlying procedures, governance and exact measures taken. Describing this institutionalisation in the context of a country's specific security environment and strategic culture supports understanding counterhybrid efforts in a more complete sense. For this purpose, strategic culture was reconceptualised. A theoretical framework was construed to examine counterhybrid efforts on the political-strategic level, organisational level, and behavioural level. Describing institutionalisation of counterhybrid efforts in this level of detail makes a structural comparison possible.

Furthermore, the second, explanatory hypothesis is: Country differences can be explained by describing geographical and societal characteristics of a country's environment together with the core elements of strategic culture, namely threat perceptions, motivations, historical practices and decision-making models. The stated descriptive and explanatory hypotheses in this paragraph and the previous one shall need to be tested in further research. A research avenue should certainly be to empirically study NATO countries as well as other country responses to hybrid threats. This article provides a framework with which this can be done, from a strategic culture viewpoint (see Table 3).

It is of course challenging to capture all real-world complexities of counterhybrid efforts in a unitary framework. A cause for this is that multiple players within one country determine counterhybrid strategy, e.g. multiple policy departments or governmental organisations. Thus, also collaborative governance arrangements need to be investigated, not merely single organisation activities taking place next to each other. This is inherently difficult. A second cause is that counterhybrid strategy, procedures, governance and measures are not always explicitly formulated. In some cases, there is no explication at all, while in other countries counterhybrid efforts can be difficult to isolate from broader national security policy. Sometimes of course, important elements of counterhybrid efforts shall also be confined to closed or secret sources due to varying reasons [35]. E.g. intelligence agency modus operandi and contributions to situational awareness as well as government deliberations on competing interests will mostly not be known openly. Thirdly, counterhybrid discourse and practice might differ. Therefore, the developed framework incorporates descriptions of high-level strategy and governance on paper as well as an examination of actual behaviour and measures taken. Thus, it is likely that inconsistencies between strategic discourse on paper and behaviour in practice are found. Fourthly, counterhybrid efforts and elements of underlying strategic culture can also change over time, although the latter will likely only change on a timescale of years or even decades. These changes create path dependencies in country responses to hybrid threats that might also explain differences between countries - when initially a country chooses a centralised response to hybrid threats, it is unlikely that full decentralisation is implemented later on. If and how well these changes can be reflected in this framework is not clear upfront. Creeping changes can occur in behaviour as well, i.e. a procedure is gradually not used anymore, whereas the procedure descriptions are still current on paper.

To further develop this research, it is necessary to actually analyse hybrid resilience and response in specific countries through the lens of strategic culture. Such cross-country case studies can demonstrate if the developed framework can be effectively used to compare and contrast, describing and explaining country differences. This future research should thus corroborate our descriptive and explanatory hypotheses as stated above. Alternatively, analysis through our framework is not enough to find and explain country differences, and explanations for differences should be found in even more drilled-down description of counterhybrid efforts and other contextual factors than a country's environment and its strategic culture. Furthermore, it would be interesting to look at changes in counterhybrid efforts over time and changes in the related aspects of strategic culture. It is unclear *a priori* what change comes first and how they relate: a change in the security environment, a change in counterhybrid tasks of organisations or a change in underlying behaviour and counterhybrid measures applied.

The proposed cross-country empirical evaluation shall also show the added value of the developed framework in practice. Another related research avenue valuable for practice would be to investigate the deterrence and defence posture of NATO as a whole against hybrid threats. Typical questions would be: What is the sum posture consisting of its country parts? How do individual country efforts interact and strengthen each other in countering hybrid threats? How do differing threat perceptions of member states negatively impact collective defence against hybrid threats? This research should not only address the benefits of international collaboration in countering hybrid threats, but also acknowledge that differences caused by elements of national strategic cultures can stand in the way of effective deterrence and defence.

6.0 CONCLUSION

The central question of this research was: What factors can be identified to explain differences between how countries counter hybrid threats? We hypothesise that countries differ in how they institutionalise their counterhybrid efforts into strategy, underlying procedures, tasks given to organisations, collaborations and exact measures they take. We also hypothesise that these differences can be explained by taking into account i) basic characteristics of a country's environment, such as the proximity of threatening hybrid actors, as well as ii) elements of strategic culture specifically applied to countering hybrid threats, including norms, ideas and practices held at the political-strategic level, organisational level and behavioural level. These hypotheses shall need to be tested in further research, mainly by empirically studying NATO country and other country responses to hybrid threats. This article provides a framework with which this can be done. The minimal added value of analysis of counterhybrid efforts by member countries is to better understand how individual hybrid response contribute pieces to the puzzle of NATO's defence and deterrence posture against hybrid threats

7.0 REFERENCES

[1] G. Giannopoulos, H. Smith and M. Theocharidou, "The landscape of hybrid threats: A conceptual model," Publications Office of the European Union, Luxembourg, 2021.

[2] NCTV, "Analysis of the hybrid threat," 05 September 2019. [Online]. Available: https://english.nctv.nl/documents/publications/2019/09/05/analysis-of-the-%E2%80%98hybrid-threat%E2%80%99-phenomenon [Accessed 21 September 2023].

[3] M. Wigell, H. Mikkola and T. Juntunen, "Best practices in the whole-of-society approach in countering hybrid threats. Study requested by the European Parliament's Special Committee on Foreign Interference in all Democratic Processes in the European Union.," European Parliament, Brussels, 2021.

[4] S. Kalniete and T. Pildegovičs, "Strengthening the EU's resilience to hybrid threats," European View, pp. 23-33, 25 March 2021.

[5] NATO, "Countering hybrid threats," NATO, 18 August 2023. [Online]. Available: nato.int/cps/en/natohq/topics_156338.htm [Accessed 10 July 2023].

[6] S. Monaghan, P. Cullen and N. Wegge, "MCDC Countering hybrid warfare project: Countering hybrid warfare," MCDC, 2019.

[7] B. Keijser, T. Powell, J. Westerveld and P. van Scheepstal, "STO Meeting Proceedings of IST-190 on Artificial Intelligence, Machine Learning and Big Data for Hybrid Military Operations," in Assessment of whole-of-society hybrid conflict: Fusion of activity signals and analyst insight, Paris, 2021.

[8] European Commission, "Joint framework on countering hybrid threats: A European Union response," European Commission, Brussels, 2016.

[9] Hybrid Centre of Excellence, "Deterring hybrid threats: A playbook for practitioners," Hybrid CoE, Helsinki, 2020.

[10] L. Lonardo, "EU law against hybrid threats: A first assessment," European Papers, pp. 1075-1096, 19 February 2021.

[11] C. Gray, "Strategic culture as context: The first generation of theory strikes back," Review of International Studies, pp. 49-69, January 1999.

[12] A. I. Johnston, "Thinking about strategic culture," International Security, pp. 32-64, 1995.

[13] A. Biava, M. Drent and G. P. Herd, "Characterizing the European Union's Strategic Culture: An Analytical Framework," Journal of Common Market Studies, pp. 1227-1248., 10 November 2011.

[14] V. Anand, "Revisiting the Discourse on Strategic Culture: An Assessment of the Conceptual Debates," Strategic Analysis, pp. 193-207, 05 September 2020.

[15] D. Zandee and K. Kruijver, “The European Intervention Initiative: Developing a shared strategic culture for European defence,” Clingendael Netherlands Institute of International Relations, The Hague, 2019.

[16] K. Wijnja, “Countering hybrid threats: Does strategic culture matter?,” Defence Studies, pp. 1-19, 26 June 2021.

[17] J. S. Lantis, “Strategic Cultures and Security Policies in the Asia-Pacific,” Contemporary Security Policy, p. 166–186, 20 June 2014.

[18] I. B. Neumann and H. Heikka, “Grand Strategy, Strategic Culture, Practise – The Social Roots of Nordic Defence,” Cooperation and Conflict: Journal of the Nordic International Studies Association, pp. 5-23, 2005.

[19] K. Kruijver, “Network governance in the international political defence realm: the case of the European Intervention Initiative,” Netherlands Defence Academy, Breda, 2020.

[20] D. G. Pantazis, “Intrastate cultural and socio-political influences and the realisation of national security: A two-level correlational analysis,” Security and Defence Quarterly, pp. 91-105, October 2021.

[21] A. Cederberg and P. Eronen, “How can societies be defended against hybrid threats?,” Geneva Centre for Security Policy (GCSP), Geneva, 2015.

[22] M. A. Kaminski and Z. Slíwa, “Poland’s Threat Assessment: Deepened, Not Changed,” PRISM, 2023.

[23] Czech Ministry of Defence, “National strategy for countering hybrid influence,” Czech Ministry of Defence, Prague, 2021.

[24] Finish Security Committee, “The security strategy for society,” The Security Committee, Helsinki, 2017.

[25] M. Bertolini, R. Minicozzi and T. Sweijs, “Ten guidelines for dealing with hybrid threats: A policy response framework,” The Hague Centre for Strategic Studies (HCSS), The Hague, 2023.

[26] Council of the EU, “Council conclusions on a Framework for a coordinated EU response to hybrid campaigns,” 21 June 2022. [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns/ [Accessed 12 June 2023].

[27] E. Pruyt and D. van Wijnmalen, “National risk assessment in The Netherlands,” in Multiple criteria decision making for sustainable energy and transportation systems, Berlin, Springer, 2010, pp. 133-143.

[28] E. Bajarunas, “Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond,” European View, pp. 62-70, 22 March 2020.

[29] B. Heap, P. Hansen and M. Gill, “Strategic communications hybrid threats toolkit,” NATO Strategic Communications Centre of Excellence, Riga, 2021.

[30] M. Rühle and C. Roberts, “Enlarging NATO’s toolbox to counterhybrid threats,” 19 March 2021. [Online]. Available: https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html [Accessed 10 July 2023].

[31] D. Zandee, S. van der Meer and A. Stoetman, "Countering hybrid threats: Steps for improving EU-NATO cooperation," Clingendael Netherlands Institute of International Relations, The Hague, 2021.

[32] G. F. Treverton, A. Thvedt, A. R. Chen, K. Lee and M. McCue, Addressing hybrid threats, Stockholm: Swedish Defence University, 2018.

[33] L. J. Morris, M. J. Mazarr, J. W. Hornung, S. Pezard, A. Binnendijk and M. Kepe, Gaining Competitive Advantage in the Gray Zone - Response Options for Coercive Aggression Below the Threshold of Major War, Santa Monica: RAND Corporation, 2019.

[34] K. Lasoen, "Realising the EU Hybrid Toolbox: opportunities and pitfalls," Clingendael Netherlands Institute of International Relations, The Hague, 2022.

[35] A. Carnegie, "Secrecy in international relations and foreign policy," Annual Review of Political Science, pp. 213-233, May 2021.