

Ambiguity or Clarity? NATO's Operational Challenge in Signalling Red Lines to Deter Hybrid Threats

Kimberley Kruijver and Neill Bo Finlayson

TNO (Netherlands Organisation for Applied Scientific Research)
Oude Waalsdorperweg 63, 2597 AK The Hague
THE NETHERLANDS

kimberley.kruijver@tno.nl, neill_bo.finlayson@tno.nl.

ABSTRACT

The effectiveness of traditional 'red lines' as tools of deterrence is increasingly undermined within the complex environment of hybrid warfare, presenting considerable challenges for NATO's operational analysis and strategic planning. Establishing conventional red lines may trigger a stability-instability paradox, wherein adversaries resort increasingly to hybrid activities.

Recent research has suggested that signalling red 'bands', rather than firm singular red lines, offers states a degree of strategic ambiguity and flexibility that is required to effectively deter a hybrid aggressor. For NATO, understanding the operational implications, strategic trade-offs, and potential escalation dynamics of these approaches is essential. As such, this paper seeks to answer the following research question: "To what extent can the concept of red bands alleviate the challenges associated with the application of red lines when deterring hybrid threats?". To answer this, a SWOT analysis of red lines versus red bands was conducted.

The results of the comparative analysis suggest that red bands are, in certain contexts, a viable and effective alternative to red lines for deterrence as long as they are being communicated clearly enough to convince adversaries of the Alliance's capability and willingness to respond. This is especially true for the vital challenge of international cooperation as every member state has their own threat perceptions and political interests. Red bands consist of multiple thresholds for unacceptable behaviour, reflecting the individual perceptions of member states, while retaining a kind of backstop for collective Alliance action with the establishment of an internationally agreed higher threshold (the red line). These findings advance research in this domain by providing insights into the development of flexible, effective and context-sensitive frameworks and strategies for establishing credible hybrid deterrence. However, more in-depth research is needed on alternative solutions to improve analytical understanding to allow decision-makers to employ nuanced, proportional counter strategies, thereby strengthening NATO's deterrence and defence posture.

1.0 INTRODUCTION

In May 2025, NATO "successfully" finished the Steadfast Deterrence exercise. Over a period of 10 days, the Supreme Headquarters Allied Powers Europe and the United States European Command simulated conflict scenarios and tested interoperability by integrating national responses (Darr, 2025). In addition, the NATO Summit that took place a month later in The Hague re-emphasised the Alliance's official deterrence and defence doctrine, by committing to a 5% defence investment to make sure that the organisation has the necessary "forces, capabilities, resources, infrastructure, warfighting readiness, and resilience" (NATO, 2025). Simply put, when deterrence of an adversary fails, NATO needs to defend itself. The large scale exercises and public communications would signal unity and willingness of the Allies to do so and thus contribute to a deterring effect.

However, it is unclear what the exact scope of that deterrence posture is and to what extent all NATO members share the same vision. It is evident from numerous overtly communicated warnings, that a clear

and unambiguous kinetic attack on a NATO ally would likely cross a ‘red line’ for the Alliance and result in Article IV consultations and invocation of NATO’s Article V. But how does this translate to the more elusive hybrid threat environment, in which the actor, the scope of their attacks as well as the effects are not always known? The earlier mentioned warnings have also been expressed in response to hybrid activities (Bajarūnas, 2025), for example when the head of the German foreign intelligence service, Bruno Kahl, said that the increase of Russian sabotage acts could prompt NATO to invoke Article 5 (Reuters, 2024). Nonetheless, this notion was quickly linked to kinetic warfare (again) as a possible future escalatory development, as Kahl referred to the option of “direct military confrontation”. Also, NATO (sometimes in cooperation with the EU) has other instruments of power to respond to attacks that remain below the threshold of armed attack stated in Article 5, including attribution, economic measures or diplomatic responses (Bajarūnas, 2024).

This paper identifies a critical area of research: evaluating the necessity and effectiveness of signalling firm red lines versus maintaining strategic ambiguity to restore deterrence and effectively respond to undesirable behaviour, within the context of international cooperation. In this area an alternative deterrence concept has arisen that matches not only the fluidity of the hybrid threat environment, but also the political complexity of multilateral decision-making: red bands (Bertolini et al., 2023). Given that the concept of red bands is novel in deterrence literature, another goal of this paper is to develop a better understanding of the concept. This paper is guided by the following research question: *To what extent can the concept of red bands alleviate the challenges associated with the application of red lines when deterring hybrid threats?* In order to answer this question, this paper draws on a diverse set of literature as well as expert input. The following chapter briefly describes the research methods, including the use of Large Language Models (LLMs) to aid in the literature search. The third chapter summarises relevant theory on deterrence, red lines and their relation to the concept of hybrid threats. The fourth chapter contains two SWOT (strengths, weaknesses, opportunities, threats) analyses, which compares the appliance of red lines and red bands when deterring hybrid threats. The fifth chapter discusses the findings by outlining different challenges for NATO that the use of red lines in the hybrid threat environment entails. The paper ends with a conclusion and future research recommendations.

2.0 METHODOLOGY

This paper is based on a mixed-methods methodology of literature review and expert input. First, the authors combined the use of LLMs with manual validation to identify relevant sources on deterrence theory in hybrid threat environments, focusing specifically on the concepts of ‘red lines’ and ‘red bands’. The process began with the use of ScholarGPT (via ChatGPT 4.5), which was prompted to find academic research meeting four criteria: relevance to hybrid deterrence, explicit use of the target concepts, scholarly credibility and recency, and high citation or policy impact. ScholarGPT returned ten articles, which were manually reviewed for relevance, access, and conceptual fit. Three were added to the database for this paper, two were considered relevant but inaccessible, and two additional sources were identified via citation snowballing. Four were excluded due to conceptual misalignment or lack of focus on hybrid threats.

Next, NotebookLM was used to expand the search by uploading two previously identified documents and issuing the same prompt. This yielded ten additional sources, including dissertations, policy briefs, and institutional reports. Gemini was then used to synthesize the gathered materials and identify further relevant literature, resulting in eight more sources, including NATO publications and legal analyses. Manual review was applied throughout to ensure quality and relevance. The combined approach allowed for efficient and broad discovery while maintaining precision through manual curation. Strengths of this methodology include rapid identification of high-quality sources, inclusion of different types of sources, and transparent selection criteria. Challenges included limited access to some materials, conceptual ambiguity in certain sources, and the time-intensive nature of manual validation.

The SWOT-method is applied to comparatively analyse the concepts of red lines and red bands. This is a systematically analytical method that helps to provide insights into devising recommendations for the future, ones that utilise existing strengths, redress existing weaknesses, exploit opportunities and protect against threats (Puyt et al., 2023). For the purposes of this paper, the strengths and weaknesses from the SWOT-categories refer to benefits and drawbacks of the *inherent* attributes of the concept of red lines and red bands in hybrid deterrence. The opportunities and threats, on the other hand, refer to the positive and negative ways in which the concept can be *exploited* or influenced by external forces. It should be mentioned that the term of 'red bands' is only literally used by one source (Bertolini et al., 2023). Therefore, arguments from a multitude of sources were used that discuss a more ambiguous and flexible application of the known concept of 'red lines'. Lastly, this paper draws on (anonymised) expert input on theoretical knowledge on deterring hybrid threats as well as on the practical reality of decision-making processes within NATO and the EU.

3.0 THEORY

Deterrence represents the strategic use of threats to persuade an adversary to abstain from a particular course of action, thereby preventing conflict by ensuring that the perceived costs of aggression outweigh any potential gains (Mallory, 2018; Van Der Putten et al., 2015; Watts et al., 2022). Effective deterrence may be achieved through the so-called "three Cs": the credibility to convincingly demonstrate both the capability and the willingness to respond; the capability to possess sufficient means to implement deterrence measures; and communication to clearly signal intent to the aggressors (Monaghan, 2022). Monaghan (2022) analyses the original requirements for deterrence as identified by Schelling (1959), which contain attribution, signalling and credibility. These factors demonstrate that the actual material capability to carry out the retaliatory threats are relatively less important than the ability to convince the adversary that the threats can and will be carried out when red lines are crossed. By combining all three C's, 'red lines' can thus be drawn.

3.1 Traditional Deterrence and Red Lines

The term 'red line' is used in different contexts in international relations to mean different things. In the context of deterrence, red lines refer to imaginative boundaries which delineate when national interests are threatened and that, if transgressed, should trigger severe consequences (Derleth & Pickler, 2022). History shows that red lines have been predominantly used by major powers to signal thresholds of unacceptable behaviour in relation to vital interests, underpinned by military strength. Such thresholds may relate to numerous things, such as military escalation, political decisions, production of sensitive materials or export of sensitive technologies (Tertrais, 2016). The term can be used to either define one's own internal position for negotiations or it can be used to externally define a threshold for action or a *casus belli* between governments (Tertrais, 2016). It is the latter that is most applicable to the context of deterrence in which red lines function as an implicit threat, its primary purpose is to deter specific actions and either maintain an existing order or establish a new status quo. In this sense, the concept of a red line, and the behaviour threshold that is signalled, inherently implies a 'point of no return', beyond which an escalatory response can be expected (Morgan et al., 2008). Tertrais (2016, p.6) offers a precise definition of red lines in the context of deterrence: "the manipulation of an adversary's intent through (mostly public) statements for deterrence purposes, referring to the deliberate crossing of a certain threshold by an adversary, and relevant counteraction if this threshold is crossed".

3.2 Deterrence in the Hybrid Threat Context

The classical understanding of deterrence as consisting of credibility, capability and communication becomes more complex when applied to hybrid threats. To effectively employ non-military means some form of international cooperation is necessary. That can be within the 'usual' intergovernmental organisations of the EU or NATO, or between multiple executive organisations like the police or even investigate journalists. Rusinaitė (2025) argues that such capabilities – which are meant to deter the foreign

actor in question – are often not communicated as such and thus do not directly contribute to deterrence. This is a big difference to conventional (nuclear) deterrence, where the mere existence of the (national) amount of for example warheads are meant to deter the adversary.

In short, it can be argued that the hybrid threat context erodes the pillars of the three C's (Monaghan, 2022; Rusinaitė, 2025). In terms of communication, it is often unclear who exactly needs to be deterred, which further complicates communication to the right target audience (Rusinaitė, 2025). Moreover, capability is eroded since hybrid adversaries generally apply innovative, cross-domain means to generate cumulative effects, which can't be fought with mere military tools. Lastly, the credibility of deterrence is undermined, since individual hybrid actions can seem insignificant. It often is their cumulative effect that have a powerful effect (Monaghan, 2022). The Hybrid Centre of Excellence (CoE) proposes three elements that might aid the erosion of the three C's against hybrid threats:

- 1) Agility, to allow rapid governmental mobilisation,
- 2) Solidarity to come up with a collective response through the EU and/or NATO, and
- 3) Attribution, which is needed to evaluate whether the measures fit the adversary actor (Keršanskas, 2020).

3.3 Red Lines in the Hybrid Threat Context

The inherent ambiguity and incremental nature of hybrid threats render traditional, rigid red lines susceptible to exploitation. Establishing conventional red lines may trigger a stability-instability paradox, wherein adversaries resort increasingly to hybrid activities (Manley, 2022). Indeed, in the age of hybrid warfare, adversaries are now adept at designing operations that precisely circumvent such thresholds (Bertolini et al., 2023), often operating just below the red lines to achieve political objectives without triggering decisive responses (Groen et al., 2025). They deliberately choose strategies to avoid crossing established red lines and exposing themselves to penalties and risks (Brands, 2016; Maass, 2025). Similarly, for the defenders of an attack or threat, it is difficult to draw red lines in the first place given the murky nature of hybrid warfare. In a context where activities, threats and actors are so ambiguous, it is hard to establish clear red lines that balance the need to deter but also to limit the risk of 'death by a thousand pricks'. Consequently, a more flexible and adaptive approach to defining boundaries is imperative. There is a considerable body of literature that discusses the development of a more strategically ambiguous implementation of red lines, with some scholars referring to this as a blurring of red lines (e.g. Faesen et al., 2020) or 'red bands' (Bertolini et al., 2023). This concept embraces a degree of strategic ambiguity, signalling to an adversary the *types* of behaviour that could trigger a response, rather than providing precise, exploitable thresholds (Bertolini et al., 2023).

This approach closely resembles the development of how NATO member states communicate and respond to hybrid attacks already. During the 2016 NATO summit in Warsaw, the Alliance affirmed that hybrid attacks could, in aggregation, meet the criteria for an armed attack under Article 5 (Lazarou & Lana, 2016), which is arguably a communication of a red line. However, the assessment for whether a hybrid attack qualifies as an Article 5 is to be done on a case-by-case basis and the operationalisation of this response is yet to be formulated (Bajarūnas, 2025). Evidently, NATO's communication on what hybrid activity elicits an Article 5 response is blurry and cannot be described as a clear red line. What specific hybrid attack, in which domain and under what circumstances would elicit the Article 5 or any other response? Is this a deliberate communication choice to leave Alliance members enough room to establish different thresholds based on the context or is this too ambiguous, leaving the adversary with plenty of attack options? With this in mind, this paper explores the complex challenges associated with the application of red lines in the hybrid threat context, while exploring the possibilities of red bands.

4.0 ANALYSIS

Based on the theory, one can reason that when a state responds to an attack by an adversary, a threshold was crossed that required a response. The question then is what kind of threshold was explicitly signalled by the defender which, therefore, dictates the kind of response that is required? In other words, how can the defender achieve a level of strategic ambiguity to ensure they are not bound to respond in a certain way, while also ensuring that credibility is maintained and the threat is deterred? The analysis below focuses on this dilemma by analysing the benefits and drawbacks of signalling *red lines* to deter hybrid threats as well as signalling *red bands*, and what the consequences are for the defender therein. As described in the methodology section, this analysis is using a SWOT-analysis structure in order to succinctly and clearly compare the operationalisation of the two concepts.

Aside from comparative strengths and weaknesses, is it also important to analyse the differences in gradation when it comes to the severity of the response. For example, if a cyber-attack has happened, and the targeted state would consequentially repair their digital systems and communicate an attribution for the cyber-attack, does that indicate the existence of a red line? Or is the response simply a standard reaction to mitigate the negative effects of an otherwise relatively minor attack? In essence, actions related to resilience building and communications are always undertaken by a state actor in response to all kinds of attacks, but also crises, accidents or other issues. Thus, to differentiate between the contravention of a red line or just a standard crisis response, this paper focuses on responses in several domains, not just those related to resilience-building and communication. Therefore, cases or examples are brought to substantiate the analysis that cover the different aspects of the DIME-FIL abbreviation. This includes actions in the following domains: diplomatic (e.g. attribution), information (e.g. counter-narratives), military (e.g. sabotage), economic (e.g. sanctions), financial (e.g. funds freezing), intelligence (e.g. identification of intelligence officers) and legal (e.g. lawfare).

4.1 SWOT Analysis: Red Lines

Strengths

The most obvious strength of red lines is the clarity of communication that it can provide. Red lines are designed to explicitly define one's interests and clearly indicate when these interests are threatened, ensuring that adversaries understand the consequences of their actions. As Derleth & Pickler (2022, p.12) explain, "effective deterrence by denial or punishment are both predicated on the elaboration of clearly defined national interests ('red lines')". Moreover, they can provide a defending country's population with reassurances of strength and resilience. For example, Finland responded to a series of suspected hybrid attacks on critical infrastructure in the Nordic region by filing charges against crew members of an oil tanker, Eagle S, suspected of causing damage to undersea cables in the Baltic Sea (Bryant, 2025; National Prosecution Authority Finland, 2025). This was supplemented by an increased presence and surveillance in the Baltic Sea by the Finnish Navy (Finnish Navy, 2025). This swift, clear and public response can be interpreted as a red line, not only acting as a deterrent for future attacks but to communicate to the public about the thresholds of activity that Finland will tolerate and the strength they have in challenging violations.

Not only do red lines communicate a clear threshold for acceptable behaviour, but they also outline the type of response that unacceptable behaviour will elicit (Morgan et al., 2008). For red lines to be truly effective, they must entail a signal that any response from the defender will be overwhelming to the adversary. If successfully communicated, such a red line has the power to prevent the kind of gradual or continual transgressions of thresholds that define the current hybrid threat landscape (Derleth & Pickler, 2022). This is the case even if the stated threshold, and associated response threat, is exaggerated – the absoluteness of signalling a red line itself can be enough to foster caution in the adversary (Schelling, 1959). The declaration of clear red lines can temporarily create what Altman (2023) describes as "windows of credibility" in which attackers fear retaliation for violations of red lines. This can have a valuable deterrent effect in the short-term regardless of whether a physical retaliation materialises or not.

Weaknesses

Communicating firm and inflexible thresholds also comes with some dangerous limitations, especially when deterring hybrid threats. Tightly defined red lines can incentivise adversaries to exploit cross-domain interconnectedness and design attacks that fall just below the red line and steer clear of specified thresholds, thereby failing to trigger a response from the defender. In essence, adversaries may see red lines as a signal that ‘anything goes’, provided that the specific red line is not crossed (Tertrais, 2016). In addition, actors can interpret the same red lines differently, therefore risking not reaching their intended objectives if the thresholds are not clear to both sides (Morgan et al., 2008). This is also a major challenge for international cooperation between allies when responding to hybrid threats. Generally, member states have different threat perceptions and thus different national security priorities which means that their formulation of a red line can differ greatly as well. This is problematic because international cooperation is vital to maintain the three Cs of deterrence (capability, credibility and communication), particularly when responding to hybrid threats where strong collaboration, intelligence sharing and coordinated responses are necessary (Wigell, 2021). Aside from the ease in which they can be circumvented by adversaries, red lines can also reduce credibility and be seen as a weakness if they are not supported through action. Repeated violations of red lines without a significant or proportionate retaliation diminish their credibility and can embolden adversaries. The Syrian red line controversy is a good example of this. It could be argued that a clear red line – Obama’s promise to intervene if chemical weapons were used in the Syrian civil war – was crossed by the Assad regime without any cost imposed, which boxed the United States into an undesirable and weak position (Ioffe, 2016; Mazarr et al., 2018). Another aspect to this is that sometimes signalling precise red lines may inadvertently reveal a state’s reaction measures and, to some extent, its internal decision systems if the signal also communicated what consequences will be applied in retaliation to violations of the red line (Derleth & Pickler, 2022).

Another fundamental weakness of red lines is what Sagan (2000) describes as the “commitment trap”. This is the dilemma in which states can be backed in to a corner from which they are forced to take certain proscribed retaliatory actions, if a declared red line is crossed, to uphold their reputation. Such a limitation on one’s freedom of action is highly undesirable, particularly if the use of physical force is on the table (Tertrais, 2016). The signalling of firm red lines that require automatic reactions therefore restricts strategic flexibility in such a way that can be detrimental in the long run. This highlights another weakness of red lines; namely, that the pressure of retaliation that comes with red lines can result in disproportionate or risky escalation.

Opportunities

On the other hand, developing and communicating red lines can play an important role in instigating the creation of international norms in the global security order. Norms can set widely accepted expectations for appropriate state behaviour, which the international community can then leverage to hold unscrupulous states accountable (Faesen et al., 2020, 2021). This is important because it broadens the scope of deterrence beyond the immediate threat and can create international consensus on certain thresholds for acceptable behaviour, thereby bolstering deterrence against future threats.

Clear red lines can be used as a viable deterrent. Although hybrid threats are often characterised by ambiguity, imprecision, incompleteness, and deniability, the signalling of tight red lines can provide some much-needed clarity on states’ interests and response measures among the murky threat environment. For instance, deterrence by punishment can effectively be supported by “clearly defined red lines for acts of aggression, particularly in the case of cyberspace, and triggers for escalation in response to non-military attacks” (Hollander, 2021, p. 3). The effectiveness here hinges on the ability to overcome the typical hurdles of verification and precise definition, allowing for a direct and decisive retaliation. The notion of overt communication of offensive cyber capabilities for deterrence suggests a move towards making the consequences of crossing such a line clear and undeniable (Bertolini et al., 2023; Neal, 2019).

Another opportunity comes from the doctrine of integrated deterrence, which states that the best use for red lines is specifically for the most dangerous cases (Derleth & Pickler, 2022). In this sense, a strict red line acts as a clear point of no return for the most critical interests, preventing an adversary from accumulating small gains into an irreversible strategic advantage. The purpose here is to deter the final, critical step that would constitute a 'fait accompli' (Monaghan, 2022). Furthermore, countries are unable to deter all hybrid threats all of the time and so the specificity of signalling red lines on particular behaviour allows defending states to focus on the most dangerous threats and protect their most exploitable vulnerabilities (Derleth & Pickler, 2022).

Threats

Adversaries can *exploit* the overly precise nature and non-enforcement of red lines to make incremental strategic gains. Red lines therefore can frustrate deterrence by enabling 'salami tactics' – incremental actions that collectively achieve a goal without provoking a major response (Bertolini et al., 2023). This is often employed as a deliberate strategy of gradual coercion and escalation in order to blur the line, and to make it politically more difficult for the defender to justify retaliation (Pierce et al., 2015). In other words, the boiling frog theory: a frog plunged in hot water will immediately jump out, but if the water temperature is raised very slowly, it may well end up being boiled (Keijser et al., 2020). This tactic is generally employed by any actor seeking to avoid a visible shock, which could mobilise governments and opinion (Tertrais, 2016). Without clear communication and credible enforcement, red lines may therefore be ineffective in deterring the full spectrum of irregular or 'grey zone' activities, potentially inviting exploitation of lower-level vulnerabilities (Derleth & Pickler, 2022). As Maass (2025, p.64) said, this can leave defenders who wish to deter hybrid aggressors without escalating matters "between a rock and a hard place".

4.2 SWOT Analysis: Red Bands

Strengths

If the strength of red lines lies in their ability to carve out clear, unambiguous boundaries, then the strength of red bands lies in their 'room for manoeuvre'. In other words, the utility of red bands lies in their ability to communicate to adversaries about unacceptable conduct while simultaneously preserving the defender's operational flexibility in crafting responses. In a complex hybrid threat environment, room for manoeuvre and interpretation may be necessary to avoid the above discussed 'commitment trap' which is a significant drawback of red lines (Tertrais, 2016). Additionally, because of their broad bandwidth, it can be argued that even if the adversary is still unknown to the defending state – which is often the case in e.g. the cyber realm, red bands could still offer the flexibility to deter, precisely because they communicate the *types* of actions which won't be tolerated.

Red bands can be communicated through both overt and covert means to inform adversaries, allies and general publics. This approach raises awareness, signals readiness, and clarifies general triggers for retaliation. Unlike red lines, red bands allow for signalling a range of thresholds – such as revealing only the highest most threshold – while keeping other details or boundaries undisclosed (Bertolini et al., 2023). As such, red bands enable the modulation of signalling. As Tertrais (2014) warns against being too sharp or too vague with communicating, red bands have the strength to only publicly establish the outer boundary while keeping over-specific inner triggers or thresholds undisclosed.

Another strength of red bands is that they are more likely to be easier to set in cooperation with like-minded partners within broader international frameworks like NATO or the EU, fostering a coalition of the willing and leveraging collective capabilities (e.g., the EU Cyber Diplomacy Toolbox) (Bertolini et al., 2023). Whereas red lines can also be set collectively, the fact that a red band consists of a spectrum of thresholds (instead of one binary threshold), allows for flexibility in terms of agreements. Therefore allies could agree on the higher threshold, but not on the lower thresholds.

Finally, red bands offer the flexibility to achieve cumulative deterrence by shaping an opponent's strategic behaviour over the long term, adapting to the iterative nature of hybrid conflict (Bertolini et al., 2023). The goal here is to gradually socialise norms of restraint. If a red band is conceptualised as a layered form of deterrence (instead of one, clear tripwire which cannot be crossed), it means that the adversary and the defending state can push and pull a little. Meaning that when an adversary does something that falls within the realm of the red band which the defending state does not like, the defending state can push them back a little with a proportionate, limited response. If the adversary then pushes back harder, the defending state still has room to escalate their response. These steps can be pre-mapped, so the defending state is prepared and knows where it can manoeuvre in terms of its responses. As such: red bands offer better escalation management as opposed to the all-or-nothing escalation of red lines (Morgan et al., 2008).

Weaknesses

The flexibility that red bands offer does come with challenges, however. The presence of multiple tiers can complicate strategic communication. Democratic deterrence depends on balancing transparency with ambiguity: publics and allies must understand commitments clearly enough to believe in them. If red bands proliferate into multiple nested thresholds, they may lose deterrent clarity and invite adversary testing (Wigell, 2021). Strategic ambiguity, if consistently communicated without evidence of supporting action, can undermine credibility over time, which erodes the deterrent effect (Bolaños, 2025; Rusinaitė, 2025; Schelling, 1959). Credibility, one of the three C's of deterrence, is therefore not a fixed attribute in an ambiguous hybrid threat environment but rather a continuously evolving perception. The defender must therefore constantly balance the benefits of strategic ambiguity with the need to provide action, without fully revealing their intentions, in order to prevent adversaries from 'calling bluff' on red bands. This is particularly relevant given that hybrid threat aggressors often pursue incremental gains through a form of coercive gradualism, a strategy where an actor gradually shifts the status quo – often using non-violent actions backed by threats – without provoking open conflict (Pierce et al., 2015). These tactics ultimately aim to capitalise on ambiguous deterrence situations (Maass, 2025; Tertrais, 2014; Wirtz, 2017).

Opportunities

Similar to red lines, red bands have the opportunity to contribute to international norm building. The difference however lies in the inherent ambiguity of red bands. The established norms would not just communicate one rigid threshold with regards to accepted behaviour, but instead layered ones. An external shared baseline could be communicated as the ultimate boundary, while different internal tiers and the associated responses could be kept covert (Tertrais, 2014). Such layered, shared baselines could be communicated through NATO communiqués, doctrines or exercises in combination with, for example, EU or UN instruments. Red bands can be used in concert with positive reassurances and incentives (economic, political, legal) and norm-setting to encourage desirable behaviour from adversaries, effectively combining deterrence with 'compellence' strategies¹ (Bertolini et al., 2023). Another opportunity would be to pair the red bands with operational indicators to make hybrid threat thresholds more observable. This could improve clarity on when thresholds within the red band are (likely to be) crossed, which could in turn improve cooperation and responding to the threats (Groen et al., 2025).

Threats

While red lines enable the threat of 'salami slicing' just *under* the communicated threshold, red bands, which consist of multiple tiers, could enable the threat of adversaries probing *within* a band. An adversary state could try to impose costs to the defending state by triggering one, but not the next tier, or the adversary could learn how to stay between these lines and present *faits accomplis* scenarios (Pierce et al., 2015; Wirtz, 2017). Repeated attacks to low-tiers of a red band, which would warrant only a modest response, could shift the perceived baselines of acceptable behaviour over time and thus erode deterrence (Groen et al., 2025; Mazarr

¹ Compellence strategies refer to "an effort to force an actor to do something" (Mazarr, 2018).

et al., 2018; Wigell, 2021). Another threat red bands could invite when they are not communicated clearly enough is when the defender's ambiguity is interpreted by the adversary as a lack of determination, motivation or credibility which in turn limits the deterrence. Furthermore, if the implementation of the red band would rely on concrete indicators, and the adversary knows that the opposing state could apply denial and deception so that the indicators would not show (preparation of) unwanted behaviour. This could lead the defending state to issue a disproportionate response (Groen et al., 2025; Morgan et al., 2008). This could lead to a second-order effect of friction between partner countries, which could be used by adversaries to create chaos and disruption to the security order.

5.0 DISCUSSION

In order to compare the two concepts, this chapter is going to plot the identified strengths and opportunities of red bands on the weaknesses and threats of red lines. By plotting these opposing elements of the SWOT analyses on each other, the table below outlines the situations in which red bands can offer an alternative to red lines. Out of seven identified challenges that can accompany applying red lines in the hybrid threat context, it is argued that one would not be solved by a red band (red), three would partly be solved (orange) and for three challenges red bands could offer a viable alternative (green).

Table 1: The challenges of red lines.

Red Line Challenges	Red Bands As Alternative?	Explanation	Examples
Signalling challenge: Actors can interpret the same red lines differently.	Partly	This also goes for red bands as this is about clear and effective communication (too vague and you lose deterrence; too precise and you lose manoeuvrability) and about different (strategic) cultures which influence perceptions.	A widely known example that clearly demonstrates this challenge, is the addition of members to the Alliance. NATO wants them to join to strengthen the Alliance to defend their joint territories. However, Russia has been interpreting this expansion as an aggression towards them.
Credibility risk: Red lines can come across as a sign of weakness if they are not supported through action.	NO	A flexible red line (thus, a red band) would also fail if it would not be enforced by action.	After European Commission President Von der Leyen's plane was jammed in September 2025, NATO Secretary-General Rutte commented that the Alliance works on it never happening again. At the same time, Bulgaria will not investigate the incident, since according to the Bulgarian Prime Minister Zhelyazkov "such things happen every day" (McNeil, 2025). Since it was just one jamming incident of an increasing trend, this could be an example of repeated warnings that are not followed up by concrete actions. This risks the loss of credibility and invitation of further attacks.

Red Line Challenges	Red Bands As Alternative?	Explanation	Examples
Commitment trap: Overly precise red lines reduce strategic flexibility.	YES	Red bands allow room for manoeuvre and strategic flexibility, helping to alleviate the problem of the commitment trap where defenders are forced to retaliate in a certain way proscribed by the red line.	The NATO 2021 Summit Communiqué stated that from then on cyber threats could “in certain circumstances” be considered an armed attack and hence invoke Article 5 (NATO, 2021). By communicating that this would be judged on a case-by-case basis, the statement could be interpreted as a red band that leaves the Alliance flexibility in their response.
Escalation pressure: Red lines can force disproportionate or risky escalation.	YES	Red bands can gradually socialise norms of restraint. As a layered form of deterrence, the adversary and the defending state can push and pull. By pre-mapping these steps, the defending state is prepared and knows where it can manoeuvre in terms of its responses. Red bands offer better escalation management.	Faesen et al. (2021) argue that actions like public attributions, indictments, sanctions, and diplomatic expulsions have been helping to form a norm protecting electoral infrastructure from cyber threats. In this sense, repeated responses are (albeit slowly) establishing a foundation to over time mitigate the targeting of the electoral process.
Just below the line: Adversaries can carry out (minor) attacks just below the threshold without direct retaliation.	YES	As opposed to one strict line, red bands signal a range of thresholds and empower the defender to be flexible and somewhat shape the adversary's behaviour.	There has been an increase in Russian sabotage actions in Europe, like break-ins at critical national infrastructure (Apps, 2024). These ‘small scale’ actions might seem insignificant alone, but they are part of a greater strategy to cause chaos and ultimately impact European cohesion and trust in governments. The actions are carried out in a way that do not necessarily individually warrant retaliations. A clear communication strategy that would signal the <i>types</i> of unacceptable behaviour could help in deterrence.
Salami tactics: Adversaries can employ incremental actions that collectively achieve a goal without provoking a major response.	Partly	Red bands can restrict an adversaries' ability to implement salami tactics <i>below</i> a threshold, but might struggle to deter attacks that cut between the lines <i>within</i> a band.	The purposeful vagueness of NATO on where the thresholds are for a cyber-attack to trigger a retaliatory response has also gotten the critique that adversaries can use this to continue with attacks. To this day, a cyber campaign has not fulfilled the

Red Line Challenges	Red Bands As Alternative?	Explanation	Examples
International cooperation challenges: It can be tricky to agree with multiple partners on what exactly 'the red line' is. International cooperation is vital to maintaining the three Cs of deterrence and underpins many other challenges.	Partly	This also goes for red bands, but red bands do offer more flexibility in this regard as they constitute layered thresholds. For example: partners could only agree on the highest threshold, but be flexible to establish individual lower ones.	criteria of the cumulative effects to warrant an Article 5 response (Bajarūnas, 2025). In practise, it would probably still be a challenge for NATO members to agree whether a specific case of cyber-attacks would warrant an Article 5 response.

One of the main findings is that the difficulties associated with international cooperation on signalling red lines symbolise NATO's challenges in deterring hybrid threats more generally. Member states have different threat perceptions and interests, which results in differences in establishing where a red line should lie. Red bands offer somewhat of a solution to this issue of alignment. For red bands, member states would need to collectively agree on the higher most threshold that would warrant an Alliance response but would retain the flexibility to establish lower intermediary thresholds to indicate when an individual state will respond or not. The band therefore consists of multiple thresholds for unacceptable behaviour, depending on the threat perception and interests of the member states, while retaining a kind of backstop for collective Alliance action with the establishment of an internationally agreed higher threshold. In this case, rather than a singular red line, a red band allows for multiple thresholds to be established before the collectively agreed 'line' is crossed.

However, the question remains whether red bands would be the most ideal approach to create a more functional hybrid deterrence. While it does provide space for manoeuvring, it doesn't necessarily support the three Cs of deterrence: communication will be vague, hence negatively influencing credibility, and (shared) capabilities are doubtful. One of the risks is that a red band might be an open invite to adversarial probing. For an adversary, it might be interesting to try things out that will hit just above the lowest threshold of one member state. The purpose would be to create a lot of debate within the Alliance, leading to disunity and consequentially result in a very weak – or entirely absent – reaction, which would then fully undermine the intended deterrence. Hence, more research is needed into other solutions to create credible hybrid deterrence, for example in the form of guaranteed responses (that have been negotiated and agreed upon within NATO before).

6.0 CONCLUSION AND RECOMMENDATIONS

The complex environment of hybrid warfare has increasingly undermined the concept of red lines as a tool for deterrence. This presents considerable problems for operational analysis and strategic planning for NATO members. By applying a comparative SWOT analysis to the concepts of red lines and red bands, this paper has evaluated to what extent the use of red bands can alleviate the challenges that come with communicating red lines. This revealed a critical dichotomy about deterrence: the strength and clarity of explicitly signalling red lines must be balanced with the need to maintain strategic ambiguity in the contemporary hybrid environment (red bands). Although this balance is required to sustain effective cross-domain deterrence, it is difficult to achieve.

Taken together, these findings suggest that red bands can, in certain contexts, be a viable and effective alternative to red lines for deterrence as long as the three Cs of deterrence are upheld. This is especially true

for the vital challenge of international cooperation as every member state has their own threat perceptions and political interests. The red band consists of multiple thresholds for unacceptable behaviour, reflecting the individual perceptions of the member states, while retaining a kind of backstop for collective Alliance action with the establishment of an internationally agreed higher threshold (the red line). This paper is a modest attempt to advance research on the use of red lines and red bands in order to develop flexible, effective and context-sensitive frameworks and strategies for establishing credible hybrid deterrence. However, more in-depth research is needed on alternative solutions to improve analytical understanding to allow decision-makers to employ nuanced, proportional counter strategies, thereby strengthening NATO's deterrence and defence posture.

7.0 BIBLIOGRAPHY

- [1] Altman, D. (2023). Red lines: Enforcement, declaration, and ambiguity in the Cuban Missile Crisis. *Journal of Strategic Studies*, 46(5), 977–1009. <https://doi.org/10.1080/01402390.2021.2004397>; PAGE:STRING:ARTICLE/CHAPTER
- [2] Apps, P. (2024, October 21). Russia's suspected sabotage campaign steps up in Europe . Reuters. <https://www.reuters.com/world/russias-suspected-sabotage-campaign-steps-up-europe-2024-10-21/>
- [3] Bajarūnas, E. (2024, November 15). Making Russia Pay for Hybrid Attacks. CEPA. <https://cepa.org/article/making-russia-pay-for-hybrid-attacks/>
- [4] Bajarūnas, E. (2025, February 11). Using NATO's Article 5 Against Hybrid Attacks . CEPA. <https://cepa.org/article/using-natos-article-5-against-hybrid-attacks/>
- [5] Bertolini, M., Minicozzi, R., & Sweijjs, T. (2023). Ten Guidelines for Dealing with Hybrid Threats A Policy Response Framework.
- [6] Bolaños, P. V. (2025). Russia's Shifting Red Lines: Nuclear Brinkmanship, Strategic Ambiguity, and the Credibility of Deterrence in Ukraine. *European Student Think Tank*, 3. <https://esthinktank.com/2025/03/03/russias-shifting-red-lines-nuclear-brinkmanship-strategic-ambiguity-and-the-credibility-of-deterrence-in-ukraine/>
- [7] Brands, H. (2016). Paradoxes of the Gray Zone – Foreign Policy Research Institute. Foreign Policy Research Institute. <https://www.fpri.org/article/2016/02/paradoxes-gray-zone/>
- [8] Bryant, M. (2025). Finland charges tanker crew members with sabotage of undersea cables. *The Guardian*. <https://www.theguardian.com/world/2025/aug/11/finland-accuses-tanker-crew-sabotage-undersea-cables-anchor>
- [9] Darr, T. (2025, June 5). NATO wraps up landmark deterrence exercise. U.S. Army. https://www.army.mil/article/286097/nato_wraps_up_landmark_deterrence_exercise
- [10] Derleth, J., & Pickler, J. (2022). Twenty-first Century Threats Require Twenty-first Century Deterrence. *Connections*, 21(2), 11–23. <https://doi.org/10.11610/CONNECTIONS.21.2.01>
- [11] Faesen, L., Klimburg, A., & Sweijjs, T. (2021). Red Lines & Baselines: Towards a European Multistakeholder Approach to Counter Disinformation. *The Hague Centre for Strategic Studies*. <https://hcss.nl/report/red-lines-baselines/>

- [12] Faesen, L., Sweijts, T., & Klimburg, A. (2020). New Report | From Blurred Lines to Red Lines: Countermeasures and Norms in Hybrid Conflict – HCSS. The Hague Centre for Strategic Studies. <https://hcss.nl/news/new-report-from-blurred-lines-to-red-lines-countermeasures-and-norms-in-hybrid-conflict/>
- [13] Finnish Navy. (2025). The Finnish Navy and allies increase presence and surveillance in the Baltic Sea – Merivoimat – The Finnish Navy. The Finnish Defence Forces. <https://merivoimat.fi/en/-/the-finnish-navy-and-allies-increase-presence-and-surveillance-in-the-baltic-sea>
- [14] Groen, M. S., Borene, A., & Livermore, D. (2025). Quantifying the Gray Zone: A Framework for Measuring Hybrid Warfare Power Balances. Small Wars Journal. <https://smallwarsjournal.com/2025/06/17/framework-for-hybrid-warfare/>
- [15] Hollander, H. (2021). Network for Strategic Analysis Policy Brief What is Grey Zone Deterrence? Network for Strategic Analysis.
- [16] Ioffe, J. (2016). The Obama Doctrine: What Did Russia Think of the “Red Line” Crisis? The Atlantic. <https://www.theatlantic.com/international/archive/2016/03/russia-syria-red-line-obama-doctrine-goldberg/473319/>
- [17] Keijser, B., Veldhuis, G., & van Scheepstal, P. (2020). Towards a Dynamic Theory of Hybrid Conflict: An Exploration with System Archetypes. In NATO Science & Technology. https://www.researchgate.net/profile/Guido-Veldhuis/publication/353972799_Towards_a_Dynamic_Theory_of_Hybrid_Conflict_An_Exploration_with_System_Archetypes/links/611ce4df1e95fe241adc3661/Towards-a-Dynamic-Theory-of-Hybrid-Conflict-An-Exploration-with-Syst
- [18] Keršanskas, V. (2020). Hybrid CoE DETERRENCE: Proposing a more strategic approach to countering hybrid threats VYTAUTAS KERŠANSKAS.
- [19] Lazarou, E., & Lana, P. (2016). The 2016 NATO Summit in Warsaw Expectations and priorities. In European Parliamentary Research Service: Briefing.
- [20] Maass, R. W. (2025). Legal Deterrence by Denial: Strategic Initiative and International Law in the Gray Zone -. Texas National Security Review, 8(3). <https://tnsr.org/2025/06/legal-deterrence-by-denial-strategic-initiative-and-international-law-in-the-gray-zone/>
- [21] Mallory, K. (2018). Perspective Expert insights on a timely policy issue New Challenges in Cross-Domain Deterrence. In RAND Corporation.
- [22] Manley, R. L. (2022). Cyber in the Shadows: Why the Future of Cyber Operations Will Be Covert. National Defense University Press. <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3105355/cyber-in-the-shadows-why-the-future-of-cyber-operations-will-be-covert/>
- [23] Mazarr, M. J. (2018). Perspective Expert insights on a timely policy issue. In RAND Corporation.
- [24] Mazarr, M. J., Chan, A., Demus, A., Frederick, B., Nader, A., Pezard, S., Thompson, J. A., & Treyger, E. (2018). What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression. RAND Corporation. <https://doi.org/10.7249/RR2451>

- [25] McNeil, S. (2025, September 2). NATO vows action as Russian GPS jamming disrupts civilian flights | AP News. <https://apnews.com/article/europe-security-russia-gps-jamming-nato-rutte-6efed7d030da19a51dfacc39ed77325>
- [26] Monaghan, S. (2019). Countering Hybrid Warfare: So What for the Future Joint Force? So What for the Future Joint Force? PRISM, 8(2), 82–99. <https://www.jstor.org/stable/26803232?seq=1>
- [27] Monaghan, S. (2022). Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice The European Centre of Excellence for Countering Hybrid Threats. www.hybridcoe.fi
- [28] Morgan, F. E., Mueller, K. P., Medeiros, E. S., Pollpeter, K. L., & Cliff, R. (2008). Dangerous Thresholds: Managing Escalation in the 21st Century. In RAND Corporation. <https://www.rand.org/pubs/monographs/MG614.html>
- [29] National Prosecution Authority Finland. (2025). Charges have been brought in the case concerning the cutting of submarine cables in the Gulf of Finland during Christmas 2024. National Prosecution Authority Press Releases. <https://syyttajalaitos.fi/en/-/charges-have-been-brought-in-the-case-concerning-the-cutting-of-submarine-cables-in-the-gulf-of-finland-during-christmas-2024>
- [30] NATO. (2021, June 14). Brussels Summit Communiqué issued by NATO Heads of State and Government (2021), 14-Jun.-2021. https://www.nato.int/cps/en/natohq/news_185000.htm
- [31] NATO. (2025, June 25). The Hague Summit Declaration. NATO. https://www.nato.int/cps/en/natohq/official_texts_236705.htm
- [32] Neal, J. (2019). Deterrence in a Hybrid Environment – per Concordiam. <https://perconcordiam.com/deterrence-in-a-hybrid-environment/>
- [33] Pierce, W. G., Douds, D. G., & Marra, M. A. (2015). Understanding Coercive Gradualism. The US Army War College Quarterly: Parameters, 45. <https://doi.org/10.55540/0031-1723.2742>
- [34] Reuters. (2024, November 27). Russian acts of sabotage may lead to NATO invoking Article 5, says German intel chief. <https://www.reuters.com/world/europe/russian-hybrid-attacks-may-lead-nato-invoking-article-5-says-german-intel-chief-2024-11-27/>
- [35] Rusinaitė, V. (2025). Turning strategy into praxis: Lessons in hybrid threat deterrence. In Hybrid Centre of Excellence. www.hybridcoe.fi
- [36] Sagan, S. D. (2000). The Commitment Trap: Why the United States Should Not Use Nuclear Threats to Deter Biological and Chemical Weapons Attacks. International Security, 24(4), 85–115. <https://www.jstor.org/stable/2539316>
- [37] Schelling, T. C. (1959). The Threat That Leaves Something to Chance. In RAND Corporation. RAND Corporation. <https://doi.org/10.7249/HDA1631-1>
- [38] Tertrais, B. (2014). Drawing red lines right. Washington Quarterly, 37(3), 7–24. <https://doi.org/10.1080/0163660X.2014.978433/ASSET/CMS/ASSET/F7D6F355-E772-46FD-841D-472998612C1A/0163660X.2014.978433.FP.PNG>
- [39] Tertrais, B. (2016). The Diplomacy of “Red Lines.” Fondation Pour La Recherche, 2.

- [40] Van Der Putten, F.-P., Meijnders, M., & Rood, J. (2015). Deterrence as a security concept against non-traditional threats. Clingendael. <http://www.clingendael.nl/>
- [41] Watts, S., Rooney, B., Germanovich, G., McClintock, B., Pezard, S., Reach, C., & Shostak, M. (2022). Deterrence and Escalation in Competition with Russia: The Role of Ground Forces in Preventing Hostile Measures Below Armed Conflict in Europe. Deterrence and Escalation in Competition with Russia: The Role of Ground Forces in Preventing Hostile Measures Below Armed Conflict in Europe. <https://doi.org/10.7249/RR-A720-1>
- [42] Wigell, M. (2021). Democratic Deterrence: How to Dissuade Hybrid Interference. *Washington Quarterly*, 44(1), 49–67. <https://doi.org/10.1080/0163660X.2021.1893027;PAGE:STRING:ARTICLE/CHAPTER>
- [43] Wirtz, J. J. (2017). Life in the “Gray Zone”: observations for contemporary strategists. *Defense & Security Analysis*, 33(2), 106–114. <https://doi.org/10.1080/14751798.2017.1310702>

