Balcaen, Pieter; Du Bois, Cindy; Buts, Caroline

Article

The hybridisation of conflict: A prospect theoretic analysis

Games

Provided in Cooperation with:
MDPI – Multidisciplinary Digital Publishing Institute, Basel

Suggested Citation: Balcaen, Pieter; Du Bois, Cindy; Buts, Caroline (2021) : The hybridisation of conflict: A prospect theoretic analysis, Games, ISSN 2073-4336, MDPI, Basel, Vol. 12, Iss. 4, pp. 1-15, https://doi.org/10.3390/g12040081

This Version is available at:
https://hdl.handle.net/10419/257563

games

MDPI

Article

The Hybridisation of Conflict: A Prospect Theoretic Analysis

Pieter Balcaen [1,*], Cind Du Bois [1] and Caroline Buts [2,*]

[1] Department of Economics, Management and Leadership, Royal Military Academy, 1000 Brussels, Belgium; cindy.dubois@mil.be
[2] Department of Applied Economics, Vrije Universiteit Brussel, 1000 Brussels, Belgium
* Correspondence: pieter.balcaen@mil.be (P.B.); caroline.buts@vub.be (C.B.)

Abstract: Revisionist actors are increasingly operationalising a broad number of non-violent threats in their quest to change the status quo, popularly described as hybrid conflict. From a defensive point of view, this proliferation of threats compels nations to make difficult choices in terms of force posture and composition. We examine the choice process associated with this contemporary form of state competition by modelling the interactions between two actors, i.e., a defender and a challenger. As these choices are characterised by a high degree of uncertainty, we study the choice from the framework of prospect theory. This behavioural–economic perspective indicates that the defender will give a higher weight and a higher subjective value to conventional threats, inducing a higher vulnerability in the domain of hybrid deterrence. As future conflict will increasingly involve choice dilemmas, we must balance threats according to their probability of occurrence and their consequences. This article raises awareness regarding our cognitive biases when making these choices.

Keywords: hybrid threats; state competition; prospect theory; grand strategy

Citation: Balcaen, P.; Du Bois, C.; Buts, C. The Hybridisation of Conflict: A Prospect Theoretic Analysis. *Games* **2021**, *12*, 81. https://doi.org/10.3390/g12040081

Academic Editors: Daniel Arce, Joao Ricardo Faria and Ulrich Berger

Received: 15 September 2021
Accepted: 18 October 2021
Published: 26 October 2021

1. Introduction

The re-emergence of long-term, strategic competition by so-called revisionist actors (i.e., states that are dissatisfied with the current distribution of power and that aim to reshape the world in their favour) such as China and Russia, constitutes one of the main contemporary security challenges [1]. Russia's aggressive actions in Ukraine in 2014 are generally seen as a tipping point, initiating an increase in the North Atlantic Treaty Organization's (NATO) budgets and putting great power competition back on top of the security agenda. The nature of this strategic competition is becoming increasingly complex. In addition to traditional conventional means, these revisionist actors are challenging the West by making use of a wide and varied range of threats across all operational domains. The competition in the informational (e.g., cyber and disinformation) and non-military domains, popularly known as 'hybrid threats', has created a grey zone where the traditional physical boundaries of conflict are eroded so that countries can be destabilised without a single soldier crossing the (physical) border [2–4]. These threats give rise to a number of challenges. While conventional conflict rarely takes place, hybrid threats occur continuously; they are more difficult to attribute to a perpetrator (who can always resort to the excuse of plausible deniability), and it is more difficult to assess the effects and the consequences associated with these types of threats.

From a defensive stance, the deterrence of this increasing number of threats gives rise to choice problems, as not only force posture but also force structure will have an impact on the national defence [5]. As power continues to diversify, political calculations must not only consider the classic trade-off between 'guns' and 'butter', as nations might have a limited number of resources available or other non-military spending priorities, but must also account for complements and trade-offs between 'guns' and 'guns' [5]. Hence, studying this form of state competition requires a shift in thinking.

As a more differentiated portfolio of options makes trade-offs more difficult, we venture in the strategic question: "How do we decide on allocating available budgetary means across different domains when striving to deter the wide range of threats we are confronted with?"

We study this broad research question by means of a traditional game theoretical deterrence model, resembling the interactions between a defender and a challenger that wishes to revise the status quo. Linked to today's international environment, the challenger represents a revisionist state such as Russia, China or North Korea [4,6,7]. The defender represents a liberal democracy, being a single individual state or an alliance of states such as NATO. The article is written from the point of view of the defender, which needs to decide upon the distribution of resources across domains. This strategic question involves a decision-making dilemma, as this choice could have large (political) consequences if deterrence in one of the domains should fail. We are therefore brought into the realm of prospect theory, standing as the leading framework for how people make choices under risk [8,9]. The subsequent integrating of elements of prospect theory into our game theoretic model therefore constitutes a good methodology to reveal how the defender will prioritise defensive capabilities when facing a wide series of threats.

Originating in the field of economics, a vast literature applies prospect theoretic findings to study several forms of conflict (see Section 3.2), serving as an alternative to the expected-utility theory. We are, however, the first to bridge the literature on hybrid conflict and the behavioural–economic literature on prospect theory. Moreover, we contribute to the growing literature on cross-domain deterrence (CDD), as our model incorporates the interactions between different domains (conventional and hybrid). This field of research focuses on the deterrence of asymmetric [10] and hybrid [11,12] threats, the use of threats in one domain to prevent actions in other domains (such as cyberspace) and the increasingly intertwined interactions between military threats and the growing portfolio of non-military threats in today's competitive environment [13].

The remainder of the article is structured as follows. Section 2 summarises the main characteristics of hybrid conflict. Section 3 recapitulates the main findings of prospect theory. Section 4 offers a prospect theoretic perspective on hybrid threats. Section 5 offers a preliminary (quantitative) discussion by analysing the U.S. budget composition. Section 6 summarises our findings and provides scope for follow-up research.

2. The Contemporary Nature of State Competition

Notions such as 'hybrid threats', 'non-linear warfare' [14] and 'grey zone conflict' [2] have received growing attention in recent years, especially following the events in Crimea in 2014. This article does not enter the semantic discussion of whether the changing way of state competition, rendered possible by an increase in technological progress (e.g., the 'internet of things' and the evolutions in artificial intelligence) and interconnectedness, can actually be described by a single definition. We use this umbrella term to cover a range of threats, because we believe they have some common characteristics that require further analysis in order to gain more insights into the dynamics of contemporary state competition. We refer to the terminology of hybrid threats as it has been adopted by NATO and the EU in their official strategic documents [15,16].

2.1. Characteristics of Hybrid Threats

First, hybrid threats refer to the combined and simultaneous use of a wide range of ambiguous, and often non-violent, means [17–19]. The most known and debated examples of hybrid threats are the spreading of disinformation (e.g., the Chinese and Russian spreading of disinformation during the COVID-19 health crisis), the foreign interference in elections, the use of cyber-attacks (e.g., the Solarwinds or Hafnium cyber-attacks targeting thousands of U.S. private firms), the targeting of critical infrastructure (e.g., the drone strikes by Iran's Houthi allies on Saudi Arabian refineries in 2019), the use of Special Forces to wage unconventional warfare (referring to the use of operations

conducted by special forces to advise and assist foreign resistance movements to conduct a resistance warfare against their host nation or occupying force [20]), the support of extreme political parties of one's opponent with the aim of increasing political polarisation (e.g., the Russian support to EU extreme right political parties) and the use of a wide range of economic instruments to exploit interdependencies (e.g., manipulating energy prices, economic aid, the use of economic sanctions such as the Russian embargoes of Ukrainian goods during the 2014 war). The seminal work 'unrestricted warfare' by the Chinese strategists Liang and Xiangsui contains a further extensive list of tools that can be used to destabilize one's adversary [21]. The effects and consequences stemming from these tools vary widely, which immediately brings us to the second characteristic associated with these types of threats.

Revisionist actors are resorting to the aforementioned means with the aim of staying below the threshold that the attacker believes would trigger an armed response. This blurs the traditional dichotomy of peace and war and is often described as fighting in the grey zone [22] or liminal warfare [8]. These threats hence enable the revisionist to inflict losses while evading a powerful international response [19,22]. This relative reluctance of Western states to respond fiercely to hybrid threats remains partly a puzzle and is often explained by referring to the difficulty of attributing the attacks to a perpetrator with sufficient certainty [2,8]. By incorporating behavioural–economic insights, our modelling provides another innovative explanation why hybrid adversaries proceed carrying out these types of intrusions, considering Western deterrent signals as incredible.

Third, the intellectual debate on hybrid conflict requires a shift from the traditional goals of conflict. Hybrid conflict is non-linear in nature and does not involve the conquest or physical control of the opponent's territory. These threats aim to create distrust towards politicians, to polarise the public debate and to weaken the sentiment of unity. This could in the longer-term lead to a gradual change of the status quo and the balance of power [23]. Our model expounds how this deterioration in the status quo can occur.

Hybrid threats clearly constitute an attractive complement to conventional capabilities, as they have a high cost-benefit efficiency. Furthermore, the increased interconnectivity and the advances in technology continue to increase the reach, efficiency and the potential to achieve substantial effects. While the aforementioned explanatory factors for resorting to these types of threats are important, they are not the subject of this article. We argue that they are also capable of exploiting the defender's cognitive pitfalls that are associated with the psychological game of deterrence [24]. Broadening the range of threats, both conventional and hybrid, forces the defender to make allocative choices, distributing available budgetary means across defence capabilities. As this allocative choice process constitutes a decision-making dilemma, we study this question from a prospect theoretic perspective, standing as the leading framework for how people make choices under risk [9,10]. We discuss the main elements of prospect theory in the following section.

3. Prospect Theory and Decision Making under Risk

Section 3.1. highlights the main findings stemming from the empirical research on prospect theory, focusing on the seminal work of Kahneman and Tversky [25,26]. Section 3.2. briefly presents the use of prospect theory within the field of international relations.

3.1. An Introduction to Prospect Theory

Prospect theory emerged as an alternative for expected utility theory when evaluating different hypothetical choices under risk, following the seminal work of Kahneman and Tversky [25,27]. Prospect theory describes a choice process, in which available options are edited in a first phase. During the subsequent evaluation phase, the option with the highest weighted value 'V' is chosen. This value is expressed as follows and depends on two distinctive functions:

$$V = \sum_{i=1}^{n} \pi(p_i) \cdot v(x_i) \quad (1)$$

$\pi(p_i)$ represents the weighting function (see Figure 1) and measures the impact of the probability of an event on the desirability of prospects. This implies that possible outcomes are weighted by a subjective decision weight $\pi(p_i)$ instead of their objective probability (p_i). Hence, this function does not necessarily represent the objective likelihood of events but rather introduces subjective probabilities. The decision weights can consequently be influenced by other factors such as ambiguity, uncertainty and risk. The weighting function bears several properties.

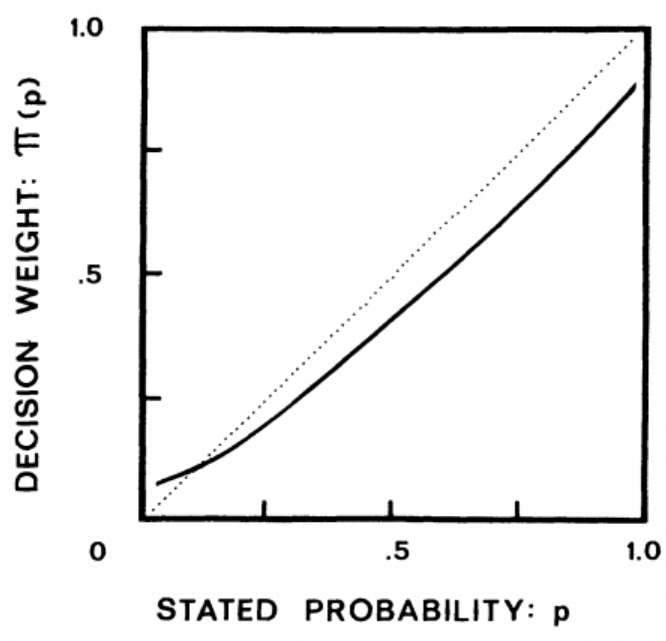

Figure 1. A hypothetical weighting function. Note: p represents the objective probability, $\pi(p)$ reflects the decision weight associated with an event. Source: Kahneman and Tversky (1979).

First, the function is not well-behaved around the endpoints, reflecting the observation that individuals face difficulties when evaluating extreme probabilities. The difference between high probabilities and certainty is therefore often neglected or exaggerated. Extremely likely but uncertain outcomes are consequently often treated as being certain, also called the pseudo certainty effect. Second, sharp increases can be observed in regions with low and high probabilities. This implies that people in general tend to overweight low probability events ($\pi(p_i) > p_i$) while underweighting high probability events ($\pi(p_i) < p_i$). Third, Figure 2 shows that probabilities are lower than unity over a large range of the weighting function, leading to the principle of subadditivity, or $\pi(p_i) + \pi(1 - p_i) < 1$, implicating that decision weights do not sum to 1 when comparing two options.

$v(x_i)$ represents the value function (see Figure 2) and assigns a value to each potential outcome, reflecting the subjective value of that outcome. This function bears some distinct characteristics. First, values are measured in terms of gains and losses that stem from deviations from a reference point. In this way, people are more sensitive to changes in wealth, rather than final asset positions. The reference point often depicts the status quo but can also be a measure of the aspiration level [28]. Second, the value function is concave for gains and convex for losses, reflecting risk averse behaviour when operating in a domain of gains and a risk acceptant behaviour with respect to losses. This implies that individuals will prefer the certain outcome instead of a gamble when operating in a gains frame, even when the gamble has a higher expected utility. Individuals operating in a loss frame will on the contrary prefer a gamble in an effort to avoid certain losses, even if the expected loss is larger. Moreover, the shape of the value function reflects the characteristic of diminishing sensitivity, indicating a decreasing marginal value of both gains and losses in terms of their magnitude. Third, the value function is steeper in the domain of losses,

reflecting the characteristic of loss aversion. The pain of loss is greater than the pleasure of gaining. Recent experiments in the field of neuroscience [29] indeed show that distinct neural circuits and activation patters are used when encoding and assessing gains or losses hereby confirming the asymmetric value function [30].

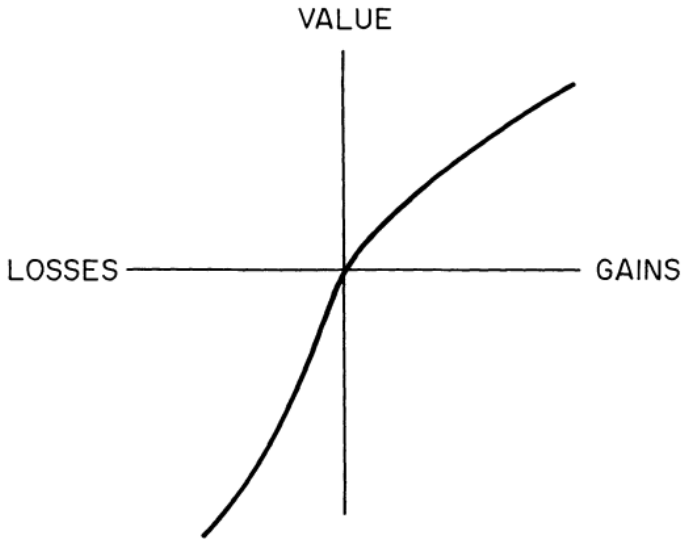

Figure 2. A hypothetical weighting function. Source: Tversky and Kahneman (1991).

3.2. The Application of Prospect Theory within the Field of International Relations

Although most of the initial research on prospect theory focuses on choices between monetary outcomes, the theory has later been applied to a wide range of decision-making problems, including the field of international relations and conflict. Next to case studies, explaining specific policy choices [31–35], the theory has been incorporated into theoretic modelling to study strategic interaction. The theory supports the revision of traditional outcomes associated with deterrence frameworks such as the chicken game [35,36], the study of great power deterrence and power cycles [37], the sequential analysis of a traditional deterrence game [38] and bargaining and ultimatum games [39]. While the list of applications of prospect theory in the field of international relations continues to grow, we are, to the best of our knowledge, the first to use the framework of prospect theory to study hybrid threats and how states respond to them.

4. Studying the Contemporary Conflict Environment from a Prospect Theoretic Perspective

We apply prospect theory to contemporary state competition, in which a defender faces a broad range of threats. Section 4.1 conceptualises this threat environment by means of a model in which the defender must deal with conventional and hybrid threats. This visualisation enables us to assess threats in terms of alternative courses of action as well as the associated outcomes and the probabilities they will occur. As these elements form the basis of 'framing' a choice problem in prospect theory [40], we heavily draw on this theory to analyse the decisions. Where Section 4.2 puts emphasis on the findings from the weighting function, Section 4.3 discusses the value function. Both functions provide corroborative insights regarding the way decision makers cope with a wide range of threats that differ strongly according to their probability of occurrence and impact. Section 4.4 discusses the challenges associated with deterring hybrid threats, by applying our findings from prospect theory.

4.1. Modelling Contemporary State Competition: The Joint Analysis of Conventional and Hybrid Threats

We present the multi-domain strategic competition between two players in Figure 3. The model is based on Balcaen et al. [41] and presents a defender (player 1) facing a challenger (player 2) that wishes to revise the status quo. We assume a unitary decision maker, in line with previous research on prospect theory within the international relations literature [9,35,38]. Further extensions such as the impact of group polarisation [42] on the decision-making process would add a further order of complexity to the model [43] and are beyond the scope of this article. It is similar to a traditional deterrence model [38,44], but allows for a variety of instruments to challenge the status quo, i.e., a combination of hybrid and conventional threats. We assume a number of simplifications. First, we differentiate between two broad categories of threats: hybrid and conventional ones, each depicted by a single branch tree. Both categories could be further expanded. The conventional domain for example could be further subdivided, making the distinction between naval, land and air forces. The hybrid branch tree could be further expanded by making a distinction between the different types of hybrid threats, e.g., disinformation campaigns, cyber-attacks, supporting proxy-forces or destabilising an opponent by means of economic coercion. We resort to this simplification because we argue that each category bears a number of similar characteristics that form the basis of the prospect theoretic analysis. Second, the deterrence game is limited to two stages and does not include retaliatory actions of the defender. We will incorporate this possibility of retaliation in Section 4.4.

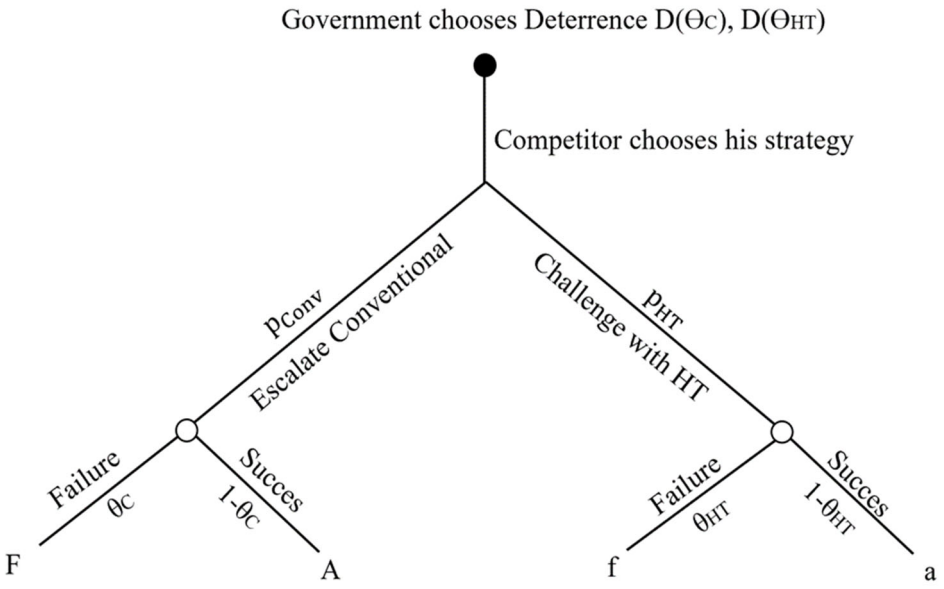

Figure 3. Interactions between a defender and a challenger (Extensive form representation). Source: simplified representation of the model presented in Balcaen et al. (2021).

The interactions between the defender and the challenger are as follows. The defender moves first and decides on the level of deterrence, making a choice between conventional deterrence $D(\theta_C)$ and capabilities that aim to deter hybrid threats $D(\theta_{HT})$. The latter can be represented as a form of *deterrence by denial* by investing in intelligence services, cyber specialists and the detection of disinformation. We specifically assume this strategy of deterrence by denial when analysing the deterrence of hybrid threats following the nature of these threats as discussed in Section 2.1, i.e., they are designed to inflict harm without justifying or provoking an armed response (i.e., punishment). We further venture in the particular discussion of deterring hybrid threats by means of a strategy of deterrence by punishment in Section 4.4. The levels of $D(\theta_{HT})$ and $D(\theta_C)$ in turn determine the challenger's perceived probabilities of failure (θ_C and θ_{HT}). These deterrence costs augment at an increasing rate in function of the failure probability. The challenger then moves and

decides how to defy his opponent, with probabilities p_{Conv} (demonstrating a conventional attack) or p_{HT} (representing the use of a hybrid threat). This probability function is assumed to be continuous with $\partial p_i/\partial \theta_j > 0$, i.e., target transference implies that efforts to counter a certain type of threat increases the probability that the challenger will revert to a different type of threat to challenge the defender. The model has four potential outcomes, i.e., a failed/successful conventional attack or a failed/successful hybrid attack. The defender strives to minimise his costs, which are composed of the foregone deterrence costs $D(\theta_C)$ and $D(\theta_{HT})$ and the costs incurred as a result of an attack. Despite the fact that hybrid attacks also have the potential to inflict severe damages (e.g., by attacking vital infrastructure, shutting down the opponent's national economy), the hybrid actor generally strives to remain under the threshold that would provoke an armed response by only inflicting limited losses. If the hybrid attack fails, the defender incurs a small cost of 'f' whereas a successful hybrid entails a cost of 'a'. Conventional conflict, on the other hand, generally results in significant human, economic and material losses. Losing the conventional attack entails a large cost 'A', winning a cost 'F', with $F < A$. The final ordering of the potential costs for the defender are $A > F > a > f$.

The focus of our analysis is not on the absolute outcomes of hybrid or conventional offensives. Instead, we focus on the choice dilemma stemming from the strong contradiction between the probabilities and outcomes that characterise these two strategies. This discrepancy between the 'probabilities' and 'impacts' associated with conventional and hybrid threats is illustrated in Figure 4. Whereas the occurrence of large-scale conventional wars between two major states constitutes a HILP event (High Impact, Low Probability), hybrid attacks occur with a high probability but entail smaller effects.

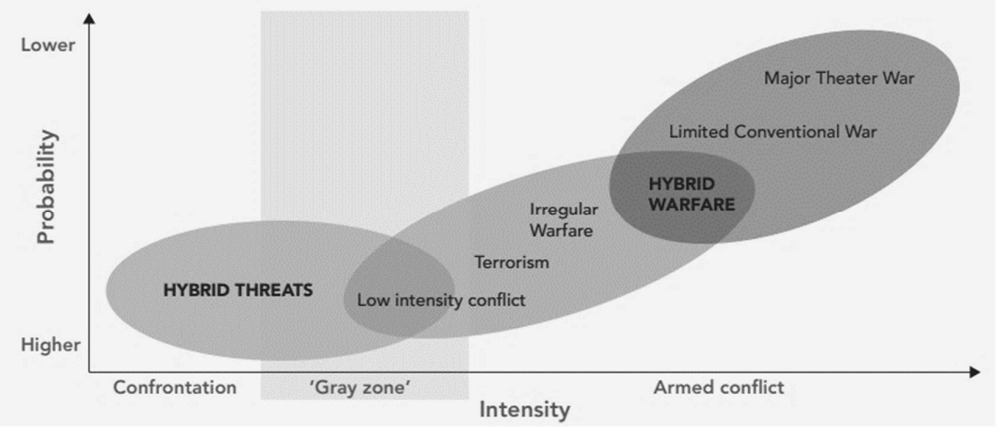

Figure 4. Probability-intensity relations across the continuum of conflict. Source: Monaghan (2019).

The defender will try to minimise his expected costs by choosing the level of deterrence $D(\theta_C)$ and $D(\theta_{HT})$. According to expected utility theory, assuming rational decision-making, the defender will balance the outcomes that are obtained by multiplying the probabilities of the different scenarios with the associated costs (the impact). However, according to prospect theory, heuristics and biases will influence the choices of the decision maker, leading to a violation of expected utility theory. The following sections incorporate the findings from prospect theory to the choice process of the defender, demonstrating the difficulty to assess the diverging prospects of conventional and hybrid conflict.

4.2. Insights from the Weighting Function

Incorporating prospect theory, the defender replaces the probabilities p_{Conv} and p_{HT} by subjective decision weights: $\pi(p_{Conv})$ and $\pi(p_{HT})$. These decision weights measure the impact of events on the desirability of prospects rather than the perceived likelihood that these events will occur [25]. This has some important implications for the weighting function.

First, as the function is assumed not to be well behaved around the endpoints, decision makers face difficulties when evaluating and responding to events that are highly likely or very unlikely. Hence, being faced with a series of threats at the extremes of the continuum of conflict complicates the decision-making process and the defining of priorities.

Second, the properties of the weighting function partially explain how we will prioritise the threats we are facing, based on the probability of occurrence. More precisely, the defender will instinctively tend to overweight low probability threats such as large-scale conventional conflict while underweighting high probability events such as the occurrence of cyber-attacks or the distribution of disinformation, or: $\pi(p_{Conv}) > p_{Conv}$ and $\pi(p_{HT}) < p_{HT}$. The overweighting of low-probability conventional conflict is further reinforced by the availability heuristic. Examples and consequences stemming from conventional conflict are widely available and come easily to mind, e.g., the images of wounded people, death or the destruction of infrastructure. They are consequently perceived as more likely than they truly are [8]. Moreover, the challenger can magnify this availability heuristic as he continues to organise nuclear tests and/or large-scale conventional exercises, by bringing its troops in a higher state of readiness and by regularly probing borders (e.g., by means of reconnaissance flights or movements of submarines). Russia, for example, gathered over 100.000 troops along the border of Ukraine and in Crimea in April 2021, signalling Putin's readiness to commit aggressive actions [45]. This signalling game further increases the subjective decision weight $\pi(p_C)$.

Third, social experiments show that the nonlinearity of the weighting function leads to a different evaluation of the complete elimination of risk as compared to the reduction of risk [25]. More specifically, individuals are willing to pay more to reduce the low probability of an event to '0' rather than obtaining the same reduction when the probability of occurring is higher. Specifically applied to our choice problem, this means that we will be more inclined to devote a higher budget to eliminate specific threats with a low probability (e.g., conventional war), while the similar reduction of threats with a higher probability (e.g., hybrid threats) is characterised by a lower 'willingness to pay'.

4.3. The Use of Hybrid Threats in Contemporary State Competition: Insights from the Value Function

In the first place, the framework of prospect theory explains why the challenger is still resorting to 'risky' actions (since the waging of hybrid attacks still entails the possibility of provoking a response that might inflict losses on behalf of the perpetrator), despite observing the deterrent measures. The challenger will defy the defender by using hybrid threats with a probability of p_{HT} since he is dissatisfied with the current status quo and perceives himself as being in a domain of losses. This motivates the challenger to risk defection as long as there is a chance that these actions will improve its situation (i.e., the benefits n_{HT} the challenger obtains). In our example, the defender can be seen as a state being satisfied with the status quo while the challenger represents a revisionist state (such as Russia, China, Iran and North Korea) that strives to change the balance of power in his favour [1,23]. Following prospect theory, deterrence becomes more difficult when potential adversaries operate in the domain of losses [35,38], as they are more willing to accept risk and to pursue confrontation. Applied to our model, this implies that higher levels of $D(\theta_C)$ and $D(\theta_{HT})$ are needed, if the defender wishes to deter the challenger across all domains. This comes at a high cost.

We now discuss how the defender assesses the different potential outcomes of the deterrence game (cfr. Figure 3). From a prospect theoretic perspective, the defender does not evaluate each outcome (A, F, a, f) as a net asset position. Instead, he assigns a subjective value to each potential outcome, i.e., the magnitude of change in relation to the asset position that serves as a reference point (in this case the status quo) [25]. We introduce the following mathematical representation of this subjective value [27,39] as it includes the variables that affect the defender's assessment of the threat environment, i.e., its degree of loss aversion (α), the degree of risk propensity (β) and the deviation from the reference point as the attack occurs (Δ). Equation (2) describes how this assessment differs upon

whether the defender perceives himself as being in a domain of gains or losses, illustrating the concave (domain of gains) and the convex (domain of losses) area of the value function (cfr. Section 3.1).

$$V_i(\Delta)\begin{cases} \Delta^{\beta} & \text{for } \Delta \geq 0 \\ -\alpha(-\Delta)^{\beta} & \text{for } \Delta \leq 0 \end{cases} \quad (2)$$

Succumbing to a conventional attack involves a large negative deviation ($\Delta << 0$) from the reference point. Following Equation (2), the subjective outcome 'A' is even further reinforced (exponentially) by the factors 'α' and 'β'. Consequently, the defender experiences a great (subjective) disutility of loss when being confronted with the consequences associated with conventional conflict. This might incite the defender to reckless actions, driven by loss aversion. A challenger that resorts to hybrid threats specifically aims to avoid these reckless responses. By pursuing actions that remain below the threshold that would trigger an armed response, he refrains from provoking a substantial negative deviation ($\Delta \approx 0$) from the reference point. In doing so, he strives to avoid being confronted with a reckless defender that attempts to recover its suffered losses.

While the effects 'a' of a single hybrid attack may be small (e.g., one single piece of disinformation), the cumulative value of the losses stemming from a high number of attacks may be substantial (e.g., the long-term effects of a well-coordinated disinformation campaign such as the Russian campaign during the 2016 U.S. elections). The feeling of loss therefore depends on the framing of the reference point: do we compare our gains or losses with respect to an initial asset position prior to a series of events (i.e., a certain number of periods ago), or do we compare our situation prior to each new individual event (i.e., the period t-1)? Comparing the status quo with a reference point in the past might reveal a greater than expected (perceived) loss. Therefore, the defender's choice of reference point and prior experiences with hybrid intrusions might have an impact on the way he evaluates the outcome of a hybrid attack. There may furthermore be a difference in evaluation between the different threats. In the U.S., where the Russian electoral interference in 2016 caused a lot of turmoil, might, for example, give a higher subjective value in future similar attempts to interfere, assigning a higher value to this particular threat.

As we depart from the model of Balcaen et al. [41], we examine whether the incorporating of prospect theory leads to diverging outcomes. Overall, we find the outcomes of the original model to be strengthened. Following Equation (2), we expect the defender to assign a higher subjective value to the outcomes of conventional conflict, whereas this holds less for outcomes associated with hybrid attacks. This further magnifies the overweighting of conventional conflict we discussed in Section 4.2, encouraging the defender to maintain (or even improve) high levels of conventional deterrence. This finding has a number of implications. First, organising a high level of conventional and nuclear deterrence is costly, absorbing large budgetary resources. As stated by Kilcullen [7] (p. 140), when referring to Russia's strategy towards the West:

> They (strategic nuclear weapons), not incidentally, served as shiny objects to distract Western intelligence analysts in an area where Western countries were then obligated to continue spending money, soaking up attention and resources even as Russia's true transformation took place in the realms of asymmetric and conventional warfare.

Furthermore, this paradoxically reduces the probability that the challenger will resort to conventional war, as the failure rate of conventional conflict becomes high. As stated by the Chinese strategists Liang and Xiansui [21], the U.S. has created a trap for itself by its dominance in the conventional domain. Confronting the U.S. in a conventional conflict would be committing suicide, leading their adversaries to resort to the use of asymmetric threats. Applied to our model, the challenger will rather increase its use of hybrid threats to challenge the opponent, as the latter has a higher likelihood of success ($1 - \theta_{HT}$). This high frequency of attacks poses numerous challenges to the defender, the most important

of which is the question: "Can these attacks be deterred?" We discuss this challenge in the following section.

4.4. The Credibility of Cross-Domain Deterrence by Punishment

As CDD essentially deals with the use of threats in one domain to deter an opponent from taking actions in another domain [13], we wonder whether high levels of conventional deterrence (cfr. Sections 4.2 and 4.3) could also serve to deter hybrid threats by means of 'deterrence by punishment'. We do so by extending the game with an additional round, giving the defender the possibility to respond as he encounters a hybrid attack. We examine the prospects of these response strategies by replacing the outcome 'successful hybrid attack' in Figure 3 with a new decision node. The defender could choose to simply accept the consequences of this attack ('no retaliation') or decide to 'retaliate'. This choice process is presented in Figure 5. Besides the sure losses of giving in (outcome 'a'), we include the potential outcomes of the retaliatory action and the associated payoffs for the defender.

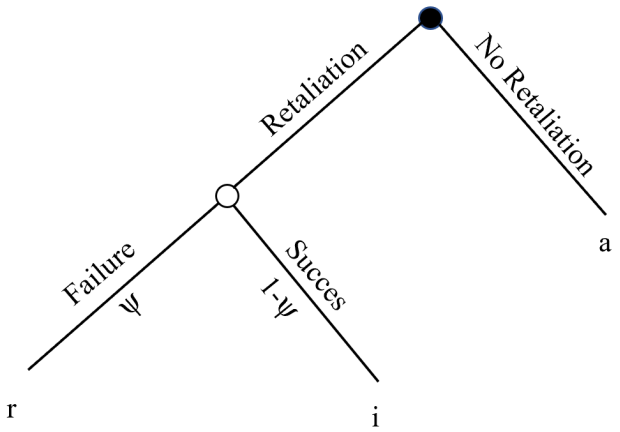

Figure 5. Retaliate or not? Choosing between two negative prospects. Source: author's own analysis.

There are two possible outcomes associated with the choice of retaliation. On the one hand, the retaliatory action could fail (taking the launching of an air raid as an example of retaliation, failing corresponds to fighter jets being intercepted or shot down), or the conflict could deteriorate even more as the challenger responds by launching counterattacks. Following Schelling [46], each act of escalation carries a degree of risk, i.e., the chance that a military action could lead to an unbearable catastrophe. This leaves the defender with the negative payoff 'r'. On the other hand, the defender's retaliatory attack could succeed, leading to gains 'i'. These gains could be interpreted as the establishment of a reputation of toughness [47], deterring future attempts to interfere in a defender's domestic country by means of hybrid threats. The defender's potential outcomes of this subgame are ordered as follows: $i > 0 > a > r$.

This represents a decision-making situation under risk, where the defender needs to make a choice between two negative prospects: (1) he does not retaliate and accepts the certain loss 'a' stemming from the hybrid attack or (2) he decides to retaliate and takes a gamble. He now has a $(1 - \psi)$ probability to improve its situation with the outcome 'i' and a (ψ) probability of losing even more 'r'. In an expected utility framework, the defender would retaliate if the following holds (in terms of expected utility):

$$\psi \cdot r + (1 - \psi) \cdot i \; > \; a \tag{3}$$

According to prospect theory, the probability of pursuing the risky option of retaliating will depend upon the defender's degree of risk propensity. The latter is, in turn, strongly influenced by the extent to which he perceives himself in a frame of loss (Equation (2)). When states perceive themselves in a domain of loss, loss aversion might lead them to

become risk acceptant. This could result in risking open conflict in an attempt to recover the suffered losses and to restore the old status quo [36,48]. However, there appears to be disagreement in the literature regarding the magnitude of decline required before an actor perceives himself in a frame of losses, leading to risk-taking behaviour. Whereas a number of authors state that only substantial losses or serious deterioration of the status quo push an actor in the loss frame [37,49], others argue that limited losses already suffice to incite states to defect [29,34,36]. Hence, the choice for 'retaliation' or 'giving in' will depend upon the defender's evaluation of the outcome, i.e., V(a). Similarly, Berejikian [35] reasons that deterrent threats over territorial disputes are not always carried out, especially when the object of dispute has limited strategic value. Under these conditions, losing this territory will not provoke retaliation as the actor that loses the territory remains in a gains frame. Following the discussion in Section 4.3, we argue that the limited losses of hybrid attacks do not suffice to incite the defender to become so risk-acceptant that he is willing to pursue retaliatory actions that could escalate and lead to catastrophic outcomes. Consequently, the defender rather evaluates the situation as follows:

$$V(\psi \cdot r + (1 - \psi) \cdot i) < 0 < V(a) \tag{4}$$

Applied to our model, the defender will therefore remain risk averse and will prefer the certain benefits from continuous cooperation to the risks associated with the scenario of retaliation which might produce even larger losses 'r'. This consequently undermines the credible communication of deterrent threats. The failure of hybrid deterrence can be easily illustrated by real world examples. The authoritarian interference tracker [50] lists a long series of hybrid attacks that occurred since 2000, making a distinction between information manipulation, cyber operations (For example the recent 'Solarwinds' and 'Hafnium' cyber-attacks that were able to target thousands of customers and public or private firms), malign finance, civil society subversion, and economic coercion. Responses to this growing list of foreign state intrusions remain limited to economic sanctions or the expulsion of diplomats at best. NATO intended to boost its deterrence posture by claiming that article 5 can be provoked in the event of a cyber-attack [51]. Despite numerous intrusions, this has not yet occurred [52].

5. Discussion

As noted in the introduction, two broad allocative decisions (that affect the allocation of means across domains) should be taken into consideration: (1) security budgets could be increased, providing additional means to invest in complementary hybrid deterrence (i.e., implying a shift from 'butter to guns'); or (2) decision makers could, given a fixed or limited budget, decide to change the defence structure (i.e., substituting 'guns by guns'. A better terminology in the framework of our model would even be to speak in terms of the allocation between 'shields', as we are looking to defend ourselves against a wide array of distinct threats). The latter trade-off implies making priorities between domains. Insights from our modelling, including the perspective of the weighting function (Section 4.2) and the value function (Section 4.3), both indicate that a defender will value conventional deterrence more. Confirming these hypotheses empirically proves, however, to be a daunting task, as there is no (declassified) granular panel data (e.g., for all NATO countries) that provides a clear overview of the break-up of military expenditures across domains.

We therefore explored this allocative question by looking at data published by one specific country, i.e., the U.S. yearly DoD request [53]. This yearly report contains an overview of the major capital expenditures across a series of categories. These categories reflect the traditional conventional domains and certain 'new' domains such as cyber. The analysis is worthwhile, as the U.S. is the country with the highest defence expenditures [54]. We do, however, readily admit that our analysis is coarse for (at least) three reasons. First, the U.S. does not merely assume the role of a defender, but also pursues other strategic objectives. Second, we are looking at input metrics, i.e., budgetary resources devoted to security. Approaching this issue through output metrics poses even greater challenges

in terms of data (it is moreover difficult to assess the 'output' of capabilities that aim to deter hybrid threats). Third, deterring hybrid threats is not a sole task for the military. In recent years, NATO and its allies have made significant efforts to provide responses to hybrid threats by establishing specialised institutions such as national cyber centres, by developing a whole of government approach (In which several agencies and ministries within a nation-state work together to counter e.g., hybrid threats [55] or by contributing to multinational centres such as the Hybrid Centre of Excellence [56]. Unfortunately, budgetary data associated with these efforts are unavailable. Hence, looking at military expenditures data only provides a partial part of the picture.

Figure 6 provides an overview of these major categorical capital expenditures over the period 2015–2021. The data shows that the conventional domains have certainly not been neglected or substituted by other domains in recent years. Both the land, air and naval domains have seen, despite the small decline in the request of 2021, a continuous increase of capital expenditures over the period 2014–2020. The maintaining of missile defence programs and tactical and strategic missiles also continues to absorb large budgetary resources. Moreover, nuclear deterrence modernisation remains a priority, costing 14 billion $ in 2020 and 28.9 billion $ in 2021. New domains such as space and cyber are however not neglected and are also steadily increased over time. This overall increase is accommodated by the increase in military expenditures.

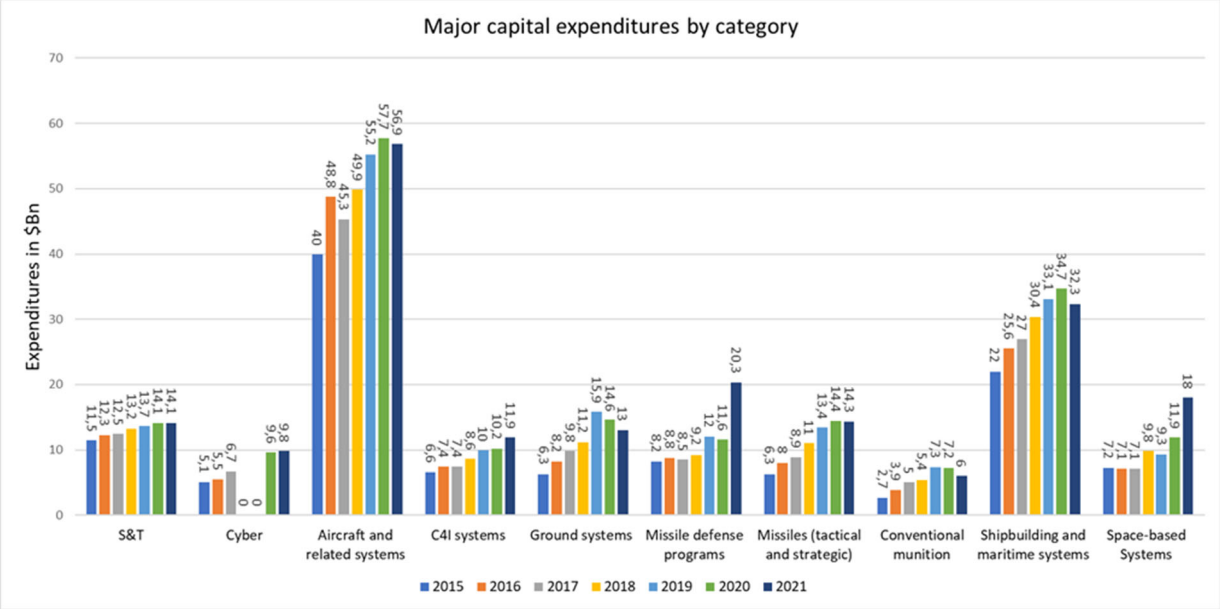

Figure 6. Major US capital expenditures by category over the period 2015–2021. Note: Values for expenditures within the cyber domain are not available for the fiscal years 2018 and 2019. Source: Own visualisation based on data from the U.S. DoD yearly budgetary request (2015–2021).

6. Conclusions and Suggestions for Future Research

The re-emergence of state competition that is being waged in an increasing number of (non-military) domains, entails difficult choices in terms of organising (cross-domain) deterrence. Not only the decision on force posture, but also on force structure could have considerable consequences upon the success rate and credibility of a nation's deterrence. We study this decision-making process by means of a deterrence model, opposing a defender and a challenger. As the defender faces a choice dilemma involving potential large strategic consequences, we incorporate findings from the leading theory of choice under risk [48], i.e., prospect theory. Both the value as the weighting function provide more insights why the defender struggles to simultaneously assess a broad range of threats that diverge strongly in terms of probability and impact. Both functions indicate that the

defender will give a higher weight and a higher subjective value to HILP events. This implies that conventional deterrence remains the above-all priority. We depart from our model to offer insights with regards to one of the main research lines within the literature on cross-domain deterrence, i.e., "Can we resort to threats in one domain (in this case the conventional domain) to deter threats that are taking place in other domains (in this case hybrid threats)?" The incorporating of prospect theoretic insights within our deterrence model provides an innovative perspective why high degrees of conventional deterrence are not credible in deterring hybrid threats.

There is no counter evidence that countries are substantially depleting their conventional capabilities to make a shift to other domains (i.e., a substitution of conventional means by hybrid deterrence). States that acknowledge the consequences associated with hybrid threats (illustrated in this article by looking at the U.S.) respond by increasing their security expenditures. This does not necessarily constitute the most optimal response strategy. As the challenger expands the competition to a larger number of domains, the defender is forced to increase its security expenditures, entailing high opportunity costs. Moreover, the increasing efforts made to face hybrid challenges remain currently insufficient. This deterrence failure can be easily illustrated by looking at the large number of (successful) hybrid intrusions that continue to occur [50,57], inflicting societal unrest and economic damages. We account the low cost and limited resources required to launch certain hybrid threats as one of the main reasons why the challenger can keep the frequency and magnitude of intrusions very high. The 'Dark Web Price Index 2020' [58] provides, for example, an overview of the cost of executing certain types of cybercrimes, estimating the cost of a DDoS attack at $10 per hour. At the same time, the cost of putting a small-to medium-sized country down for an hour is estimated at $5600 per minute. We assess that this will render it more and more difficult for the defender to remain superior in all domains and to fend off all attacks at an acceptable (societal) cost. It remains to be seen who will prevail in this competitive race. As the defender must make difficult choices, this article raises awareness of our cognitive biases.

Taking the theoretic model proposed in this article as a starting point, we acknowledge that further qualitative and quantitative research is required to test and improve our understanding of hybrid threats and to optimise our policy responses. We offer two specific recommendations, in line with previous empirical research on prospect theory in a context of conflict. First, future research could confront test subjects (e.g., decision makers such as politicians, or regular citizens if we want to assess how the public evaluates these threats) with hybrid threat scenarios that involve hypothetical policy responses and different outcomes. This methodology, in line with earlier research on other forms of conflict [9,42,59], allows to identify the degree of loss aversion and the types of events that trigger a response, i.e., which events produce a subjective feeling of loss that makes us more risk acceptant? It might be particularly interesting to compare policy responses against various reference points that are framed differently, i.e., with respect to the asset position at the beginning of a series of choices (going back in time) or with respect to the asset position at each individual choice. Second, as hybrid attacks occur frequently, we can conduct large-N statistical analyses [29]. This is, however, resource and time consuming. Although a (non-exhaustive) list of hybrid attacks can be easily obtained (e.g., the authoritarian interference tracker), this is not the case for the policy responses. Identifying these responses requires additional qualitative research such as the analysis of policy documents, statements and interviews. A particular challenge lies in the identification of the reference point prior to being exposed to hybrid threats [43]. These findings can help to increase the credibility of our resolve towards hybrid threats and the delineation of red lines in current great power state competition.

Author Contributions: Conceptualisation, P.B.; methodology, P.B.; validation, C.D.B. and C.B.; formal analysis, P.B., C.D.B. and C.B.; writing—original draft preparation, P.B.; writing—review and editing, C.D.B. and C.B.; supervision, C.D.B. and C.B. All authors have read and agreed to the published version of the manuscript.

Funding: This article did not receive any external funding.

Data Availability Statement: See citations in the text and the reference list.

Acknowledgments: We thank Marc Jegers, Daniel Arce and Edward Hunter Christie for comments on earlier drafts. We also thank the participants of the 2021 International Conference on Economics and Security for their valuable feedback. An earlier version of this article was awarded the "Michael D. Intriligator Student Fund" following the presentation during the 2021 International Conference on Economics and Security.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. US Department of Defense. Summary of the 2018 US National Defense Strategy. Available online: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (accessed on 25 May 2021).
2. Pettyjohn, S.L.; Wasser, B. *Competing in the Grey Zone*; The Rand Corporation: Santa Monica, CA, USA, 2019. Available online: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2791/RAND_RR2791.pdf (accessed on 10 June 2021).
3. NATO. NATO 2030: United for a New Era: Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General. Available online: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf (accessed on 10 March 2021).
4. NATO. Annual Report 2020. Available online: https://www.nato.int/cps/en/natohq/opinions_182236.htm (accessed on 24 April 2021).
5. Lindsay, J.R.; Gartzke, E. Politics by many other means: The comparative strategic advantages of operational domains. *J. Strateg. Stud.* **2020**, 1–34. [CrossRef]
6. Coats, D.R. Worldwide Threat Assessment. US Intelligence Community. 2019. Available online: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (accessed on 15 June 2021).
7. Kilcullen, D. *The Dragons and the Snakes, How the Rest Learned to Fight the West*; Oxford University Press: Oxford, UK, 2020.
8. Levy, J.S. An introduction to prospect theory. *Political Psychol.* **1992**, *13*, 171–186.
9. Berejikian, J.D.; Zwald, Z. Why language matters: Shaping public risk tolerance during deterrence crisis. *Contemp. Secur. Policy* **2020**, *41*, 507–540. [CrossRef]
10. Knopf, J.W. The fourth wave in deterrence research. *Contemp. Secur. Policy* **2010**, *31*, 1–33. [CrossRef]
11. Mallory, K. *New Challenges in Cross-Domain Deterrence*; The Rand Corporation: Santa Monica, CA, USA, 2008. Available online: https://www.rand.org/pubs/perspectives/PE259.html (accessed on 15 June 2021).
12. Sweijs, T.; Zilincik, S. *Cross Domain Deterrence and Hybrid Conflict*; The Hague Center for Strategic Studies: the Hague, The Netherlands, 2019. Available online: https://hcss.nl/report/cross-domain-deterrence-and-hybrid-conflict (accessed on 29 April 2021).
13. Lindsay, J.R.; Gartzke, E. *Cross-Domain Deterrence: Strategy in An Era of Complexity*; Oxford University Press: Oxford, UK, 2019.
14. Galeotti, M. Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? *Small Wars Insur.* **2016**, *27*, 282–301. [CrossRef]
15. Caliskan, M.; Liégeois, M. The concept of 'hybrid warfare' undermines NATO's strategic thinking: Insights from interviews with NATO officials. *Small Wars Insur.* **2020**, *32*, 295–319. [CrossRef]
16. Giannopoulus, G.; Smith, H.; Theocharidou, M. *The Landscape of Hybrid Threats: A Conceptual Model*; The Hybrid Centre of Excellence: Helsinki, Finland, 2020. Available online: https://op.europa.eu/en/publication-detail/-/publication/b534e5b3-7268-11eb-9ac9-01aa75ed71a1 (accessed on 15 June 2021).
17. Chivvis, C. *Understanding Russian 'Hybrid Warfare' and What Can Be Done about It*; The RAND Corporation: Santa Monica, CA, USA, 2017. Available online: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf (accessed on 30 June 2021).
18. Seely, R. Defining contemporary Russian warfare: Beyond the hybrid headline. *RUSI J.* **2017**, *162*, 40–49. [CrossRef]
19. Monaghan, S. Countering hybrid warfare. *PRISM* **2019**, *8*, 82–99.
20. Kilcullen, D. The evolution of unconventional warfare. *Scand. J. Mil. Stud.* **2019**, *2*, 61–71. [CrossRef]
21. Liang, Q.; Xiangsui, W. *Unrestricted Warfare*; Foreign Broadcast Information Service (FBIS); PLA Literature and Arts Publishing House: Beijing, China, 1999.
22. Hoffman, F. Examining complex forms of conflict: Grey zone and hybrid challenges. *PRISM* **2019**, *7*, 30–47.
23. Radin, A.; Reach, C. *Russian Views of the International Order*; The Rand Corporation: Santa Monica, CA, USA, 2017. Available online: https://www.rand.org/pubs/research_reports/RR1826.html (accessed on 25 May 2021).
24. Bijlsma, T. What's on the human mind? Decision theory and deterrence. In *Netherlands Annual Review of Military Studies 2020*, 1st ed.; Osinga, F., Sweijs, T., Eds.; Springer: Berlin, Germany, 2020; pp. 437–454.
25. Kahneman, D.; Tversky, A. Prospect theory: An analysis of decision under risk. *Econometrica* **1979**, *47*, 263–291. [CrossRef]

26. Tversky, A.; Kahneman, D. Loss aversion in riskless choice: A reference-dependent model. *Q. J. Econ.* **1991**, *106*, 1039–1061. [CrossRef]
27. Tversky, A.; Kahneman, D. Advances in prospect theory: Cumulative representation of uncertainty. *J. Risk Uncertain.* **1992**, *5*, 297–323. [CrossRef]
28. Heath, C.; Larrick, R.P.; Wu, G. Goals as reference points. *Cogn. Psychol.* **1991**, *38*, 79–109. [CrossRef]
29. Berejikian, J.D.; Early, B.R. Loss aversion and foreign policy resolve. *Political Psychol.* **2013**, *34*, 649–671. [CrossRef]
30. Litt, A.; Eliasmith, C.; Thagard, P. Neural affective decision theory: Choices, brains and emotions. *Cogn. Syst. Res.* **2008**, *9*, 252–273. [CrossRef]
31. Farnham, B. Roosevelt and the Munich crisis: Insights from prospect theory. *Political Psychol.* **1991**, *13*, 205–235. [CrossRef]
32. Richardson, L. Avoiding and incurring losses: Decision-making in the Suez crisis. *Int. J.* **1992**, *47*, 370–401. [CrossRef]
33. McDermott, R. Prospect theory in international relations: The Iranian hostage rescue mission. *Political Psychol.* **1992**, *13*, 237–263. [CrossRef]
34. Haas, M.L. Prospect theory and the Cuban missile crisis. *Int. Stud. Q.* **2001**, *45*, 241–270. [CrossRef]
35. Berejikian, J.D. A cognitive theory of deterrence. *J. Peace Res.* **2002**, *39*, 165–183. [CrossRef]
36. Berejikian, J.D. Model building with prospect theory: A cognitive approach to International Relations. *Political Psychol.* **2002**, *23*, 759–786. [CrossRef]
37. Tessman, B.F.; Chan, S. Power cycles, risk propensity and great power deterrence. *J. Confl. Resolut.* **2004**, *48*, 131–153. [CrossRef]
38. Carlson, L.J.; Dacey, R. Sequential analysis of deterrence games with a declining status quo. *Confl. Manag. Peace Sci.* **2006**, *23*, 181–198. [CrossRef]
39. Butler, C.K. Prospect theory and coercive bargaining. *J. Confl. Resolut.* **2007**, *51*, 227–250. [CrossRef]
40. Tversky, A.; Kahneman, D. The framing of decisions and the psychology of choice. *Science* **1981**, *211*, 453–458. [CrossRef] [PubMed]
41. Balcaen, P.; Du Bois, C.; Buts, C. A game-theoretic analysis of hybrid threats. *Def. Peace Econ.* **2021**, 1–16. [CrossRef]
42. Boettcher, W.A. The prospects for prospect theory: An empirical evaluation of international relations applications of framing and loss aversion. *Political Psychol.* **2004**, *25*, 331–362. [CrossRef]
43. Stein, J.G. The micro-foundations of international relations theory: Psychology and behavioral economics. *Int. Organ.* **2017**, *71*, S249–S263. [CrossRef]
44. Zagare, F.C.; Kilgour, M.D. Asymmetric deterrence. *Int. Stud. Q.* **1993**, *37*, 1–27. [CrossRef]
45. Roth, A.; Harding, L. Russia to Pull Back Troops from Crimea and Ukraine Border. The Guardian. Available online: https://www.theguardian.com/world/2021/apr/22/russia-to-pull-back-troops-from-crimea-and-ukraine-border (accessed on 10 June 2021).
46. Schelling, T. *The Strategy of Conflict*; Harvard University Press: Cambridge, UK, 1960.
47. Nalebuff, B. Rational deterrence in an imperfect world. *World Politics* **1991**, *43*, 313–335. [CrossRef]
48. Levy, J.S. Loss aversion, framing, and bargaining: The implications of prospect theory for international conflict. *Int. Political Sci. Rev.* **1996**, *17*, 179–195. [CrossRef]
49. Levy, J.S.; Whyte, G. A cross-cultural exploration of crucial decisions under risk: Japan's 1941 decision for war. *J. Confl. Resolut.* **1997**, *41*, 792–813. [CrossRef]
50. Alliance for Securing Democracy. The Authoritarian Interference Tracker. Available online: https://securingdemocracy.gmfus.org/hamilton-dashboard/ (accessed on 20 June 2021).
51. NATO. Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference. Available online: https://www.nato.int/cps/en/natohq/opinions_154462.htm?selectedLocale=ru (accessed on 15 March 2021).
52. Leuprecht, C.; Szeman, J.; Skillicorn, D.B. The damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. *Contemp. Secur. Policy* **2019**, *40*, 382–407. [CrossRef]
53. US Department of Defense. US Defense Budget Overview. Available online: https://comptroller.defense.gov/Budget-Materials/ (accessed on 10 June 2021).
54. Stockholm International Peace Research Institute (SIPRI). Military Expenditures Database 2020. Available online: https://www.sipri.org/databases/milex (accessed on 28 June 2021).
55. Cami, G.; Shea, J.; Mikaela d'Angelo, M.; Huerta, G.; André, L.; Arenella, R.; Lów, E. *Hybrid and Transnational Threats*; Friends of Europe: Brussels, Belgium, 2018. Available online: https://www.friendsofeurope.org/wp/wp-content/uploads/2019/04/FoE_SEC_PUB_Hybrid_DP_WEB.pdf (accessed on 15 March 2021).
56. Hybrid Centre of Excellence. What Is the Hybrid CoE? Available online: https://www.hybridcoe.fi/about-us/ (accessed on 18 March 2021).
57. Council on Foreign Relations. Cyber Operations Tracker. Available online: https://www.cfr.org/blog/new-entries-cfr-cyber-operations-tracker-q4-2020 (accessed on 1 July 2021).
58. Mission Critical. The Dark Web: DDoS Attacks Sell for as Low as $10 Per Hour. 2020. Available online: https://www.missioncriticalmagazine.com/articles/93185-the-dark-web-ddos-attacks-sell-for-as-low-as-10-per-hour (accessed on 2 July 2021).
59. Kertzer, J.D. Resolve, time and risk. *Int. Organ.* **2017**, *71*, S109–S136. [CrossRef]