TNO

The Hague Centre for Strategic Studies

HCSS Security

A Framework for Cross-Domain Strategies Against Hybrid Threats

Tim Sweijs, Samuel Zilincik, Frank Bekkers & Rick Meessen

Table of Contents

List of Figures 2

List of Tables 2

Executive Summary 3

1 Introduction 14

2 Strategic Framework to Counter Hybrid Action 15

2.1 Scope of the Framework: Beyond Deterrence as a Catch-All Term 15

2.2 A Framework of Strategies 18

2.3 Vertical Escalation: Five Levels on the Escalation Ladder 22

2.4 Horizontal Escalation: the DIMEL Domains 23

3 Concrete Measures for Strategies In DIMEL domains 27

3.1 Diplomatic Domain 27

3.2 Information Domain 29

3.2.1 Information Content 29

3.2.2 Information Infrastructure (Cyber Domain) 33

3.3 Military Domain 36

3.4 Economic Domain 38

3.5 Legal Domain 40

4 From Single Domain To Cross-Domain Strategies: Issues to Consider 42

4.1 Cost-Benefit Assessment 42

4.2 Cross-Domain Orchestration Assessment 43

4.3 Proportionality Assessment 43

4.4 Signaling Assessment 44

4.5 Legal and Normative Frameworks Assessment 44

4.6 Insights for the HCDS Game 45

4.7 Conclusion 46

Bibliography 48

List of Figures

Figure 1: Strategies and an escalation ladder 6
Figure 2: Cross-domain escalation 7
Figure 3: Combining instruments of power in hybrid conflict 8
Figure 4: Intrinsic horizontal escalation hierarchy of the DIMEL domains 9

List of Tables

Table 1 A framework of strategies 4
Table 2 From Single Domain to Cross-Domain: Issues to Consider 12
Table 3 A framework of strategies 18
Table 4 Diplomatic measures 28
Table 5 Information (content) measures 32
Table 6 Cyber measures 36
Table 7 Military measures 38
Table 8 Economic measures 39
Table 9 Legal measures 41
Table 10 Five kinds of assessment in the formulation, selection and execution of cross-domain strategies 46

Executive Summary

The Netherlands, together with likewise partners in its network of alliances, requires a strategic posture in an era of hybrid conflict. A strategic posture refers to the set of dominant strategies that make up a state's security policy to achieve a set of objectives. It is guided by an overarching purpose and objectives (ends) and offers general guidelines as to how to act and react (ways), thus providing guidance for the development of capabilities (means). In the case of hybrid threats, a strategic posture can:

- assist in defining and preparing the pre-requisites for counter hybrid action in terms of capabilities, legal and doctrinal frameworks, and mandate allocation;
- be instrumental in creating unity of action and synergy between counter hybrid measures by tying them together in one coherent whole;
- help in communicating to opponents and allies what are considered to be acceptable forms of hybrid behavior. It can thereby be instrumental in the development of international norms that limit hybrid threat behavior; and
- thus ultimately shape the cost calculus of an adversary which in turn can prompt changes in adversarial behavior.

This report serves as a background document to prepare a hybrid conflict game organised in the winter of 2020 by TNO in collaboration with HCSS to gain a better understanding of how cross domain strategies can help in countering hybrid threats. It presents a strategic framework that describes and explains relationships between strategies and counter-strategies in dealing with hybrid threats; and offers a number of considerations to select those dominant strategies that are to be part of the Dutch strategic posture. It does so in the understanding that a strategic posture is dynamic in nature because the evolving character of challenges requires adaptiveness.

Scope of the framework

Many contemporary ideas on countering hybrid threats draw inspiration from a larger body of thought on deterrence. Hybrid threats are difficult to prevent through deterrence alone for an assortment of reasons. In a globally connected, multipolar security environment, technological developments have contributed to the democratization of the means of violence. This, at least in some cases, favors the offensive and renders deterrence unstable. Furthermore, by their very nature, hybrid actions are not always easily attributable which undermines deterrence. Some authors have also pointed to the overall declining payoffs associated with the manipulation of fear across a variety of domains which can be partially extrapolated to the security domain. Finally, our understanding of the role of psychology and perceptions has progressed to such a degree that it is necessary to broaden the framework to include influence strategies to dissuade but also persuade adversaries beyond deterrence alone. This brings us full circle back to insights already coined in the traditional deterrence

literature which defines deterrence as "a process of influencing the enemy's intentions, whatever the circumstances, violent or non-violent."[1]

The framework's two axes

In recognition of the above, our framework consists of two axes to differentiate between the range of strategies that can be applied against hybrid threat actors. The combination of the two axes gives a full conceptual range of types of strategies to apply in a hybrid threat context. Our framework explicitly draws on and extends the survey of King Mallory on different strategies in his analysis of cross domain deterrence from 2018.[2]

Vertical (de-)escalation options

The vertical axis consists of five general strategies: cooperation, persuasion, protection, coercion, and control (see Table 1). These five strategies differ in the appliance of sticks or carrots in order to influence the behavior of the other party, as explained below.

Strategy	Description
Cooperation	The pursuit of reciprocally beneficial policies to maximize mutual gains for both the source and the target
Persuasion	The use of rewards to achieve cooperation from the target
Protection	The increase of the source's capability to withstand or absorb hostile measures
Coercion	The use of threats to prevent or change the target's behavior
Control	The use of force to limit the target's freedom of action

Table 1 A framework of strategies

Cooperation is the pursuit of reciprocally beneficial policies to maximize mutual gains for both the source and the target through entanglement, conciliation and accommodation.[3] Entanglement typically takes the form of creating mutual dependencies, usually economic or supply-chain based, whose disruption would reciprocally harm both actors and thus disincentivize destabilizing actions. Conciliation refers to removing key obstacles to reaching an agreement, without agreeing to a major part of the other side's demands. This mode of negotiation seeks a win-win solution rather than win-lose or zero-sum distributive bargaining. Accommodation involves minor concessions from one side (although they may be communicated as substantial concessions to the target) to achieve agreement. The

[1] Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security.*, First Edition (Princeton: Princeton University Press, 1961), 11.
[2] King Mallory, 'New Challenges in Cross-Domain Deterrence', (Santa Monica: RAND Corporation, 2018), https://www.rand.org/pubs/perspectives/PE259.html.
[3] 'Source' refers to the actor taking a measure and 'target' to the intended recipient or audience of the measure. Of course, in an action-reaction sequences, measures provoke countermeasures in which 'source' and 'target' are reversed.

crucial caveat is that cooperation requires reciprocal good faith. Absent that, the other party can exploit a cooperative strategy to achieve its own objectives or revert to confrontational distributive bargaining. Cooperation can enhance protective and persuasive strategies. It may stack with coercion but is unlikely to work well alongside control.

Persuasion uses rewards to achieve cooperation from the target, as an alternative for continued confrontation. It requires some goodwill on the part of the target; and thus a pause or reversal of escalatory actions, as well as effective communication to convey overtures by which a target can reciprocate without being seen to lose legitimacy or capitulate. Successful persuasion leads to win-gain scenarios. Material forms of persuasion include economic inducements or other tangible rewards. Immaterial forms include the prospects of status, prestige, good relations or credible reassurances about the other's security. Persuasion may be combined with some form of coercion or of cooperation. Persuasion does not work well alongside control strategies because it loses much of its credibility when unilateral violence is introduced into the equation.

Protection aims to increase of the source's capability to withstand or absorb hostile measures and typically results in win–zero scenarios. The two basic forms of protection are resilience and defense. The function of defense is to thwart attacks, while the function of resilience is to mitigate its consequences. Both resilience and defense can be conducted across all sectors and domains. The main purpose of both is to deal with the actual hostile measures. Yet, if they are strong, they can also help to dissuade a target from carrying out hostile measures because the target will not yield expected benefits. This gives protective strategies the potential to enhance deterrence methods. For all these reasons, both forms of protection need to be constantly updated to keep pace with the most recent character of the threat.

Coercion, in contrast to the reward-centric cooperation and persuasion, conveys persuasion to adversaries via negative means. It compels another actor to do something it does not want to do through deterrence and compellence. The former entails the use of threats to dissuade the target from taking a particular action, the latter to convince the target to take a particular action. Successful coercion typically results in win-lose scenarios. Examples span the range of sanctions regimes, bilateral diplomacy, and the use of cyber and hybrid tools, as the use of explicit military tools of coercion has been reduced by (most) actors in modern times. Coercive strategies can also be conducted by threats of shaming or stigmatization. Unlike protective strategies, coercive strategies target specific adversaries for specific ends. This implies that threats need to be tailored to the character of the target and the intended change of behavior. Therefore, the conduct of coercive efforts needs to be rooted in a clear understanding of one's vulnerabilities and of the character of the hostile measures, as well as a detailed understanding of the desired change in behavior one wishes to induce. Failure to do so may lead to miscommunication, provocation and escalation.

Control refers to the use of force to limit the target's freedom of action. Successful control typically leads to win-defeat scenarios. Control strategies involve prevention or preemption. The former uses active measures that degrade the target's capability to pose a threat before it has become imminent; the latter forcefully eliminates immediate threats. Both are aimed at specific adversaries. The major risk of control is that it may increase rather than decrease the target's willingness to implement hostile measures in response to an attack. In other words, control may as much provoke attacks as it can prevent them.

These five strategies can be used simultaneously or sequentially. In both cases, strategies should be used carefully to rectify each other's deficiencies and to enhance their potential. Some strategies, such as cooperation and protection, always amplify each other's potential. Other strategies, such as control and persuasion will undermine each other if used in tandem. All strategies contain some limitations and risk of failures and therefore no single element may constitute a singular means of ensuring security.

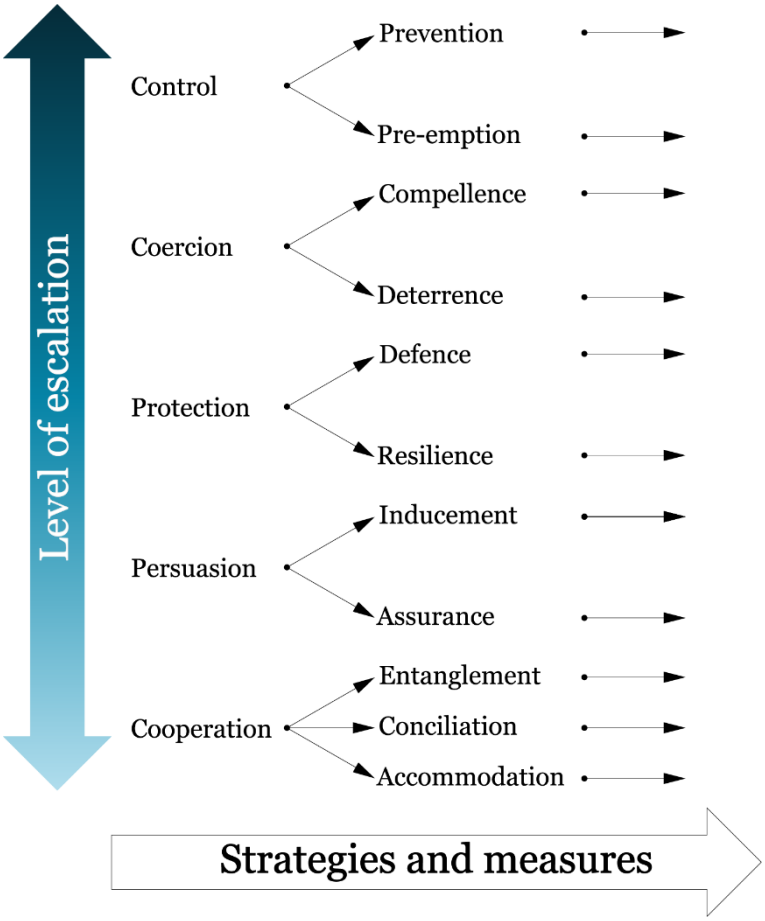

Figure 1: Strategies and an escalation ladder[4]

[4] The visual is an adaptation and extension of the visual developed by King Mallory, see King Mallory, 'New Challenges in Cross-Domain Deterrence', (Santa Monica: RAND Corporation, 2018), https://www.rand.org/pubs/perspectives/PE259.html.

The five strategies can be plotted on an escalation ladder, a spectrum from the least escalatory to most escalatory measures (see Figure 1). Escalation refers to an increase in the intensity or scope of conflict that crosses the threshold(s) considered significant by one or more of the participants. The escalation ladder represents a metaphor in crisis management in which actors can take steps to manage the intensity of the conflict, either through the escalation, de-escalation or a combination of the two via different channels in order to communicate with an adversary. All strategies can be used for both escalatory and de-escalatory purposes *except* cooperation, which by definition leads to de-escalation. This also implies that strategies should be employed carefully to augment each other's (de)escalatory potential rather than hinder, or in the case of using control and persuasion strategies simultaneously, undermine each other. If one seeks escalation, then it does not make sense to use cooperation alongside coercion and vice versa. The common denominator between strategies must be recognized in their utilization across domains.

Horizontal (de-)escalation options

In addition to vertical (de-)escalation options, one can also escalate horizontally (see Figure 2). For this, the framework uses the well-known DIMEL categorization of instruments and measures of state power, distinguishing between Diplomatic, Information, Military, Economic, and Legal domains. Vertical measures convey escalation within the same domain. For example, if hostile measures revolve around cyber espionage, a vertically escalating response may include acts of cyber sabotage. In contrast, horizontal escalation refers to broadening the scope of efforts beyond a single DIMEL domain to other domains. For instance, diplomatic and economic sanctions can be used in response to military aggression, as the West did in the aftermath of the Russian annexation of Crimea. One level deeper, horizontal escalation can also take place within various military domains. Israel, for instance, used airstrikes against Hamas in the spring of 2019 in retaliation for a series of cyberattacks, utilizing a kinetic countermeasure to a cyber threat.

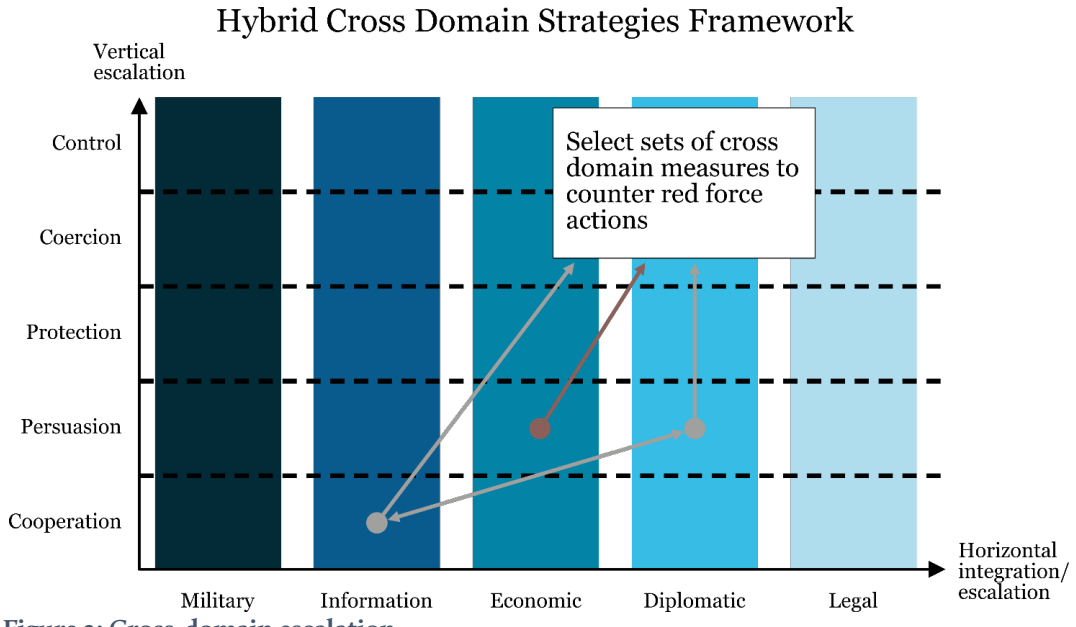

Figure 2: Cross-domain escalation

In hybrid conflicts, actors not only switch between domains but also combine the different power instruments while varying the level of intensity per domain (see Figure 7). By doing so, hybrid actors typically move up and down the escalation ladder in what is called the grey zone between war and peace, while avoiding the threshold that would lead to open (military) conflict. In addition, hybrid tactics leverage conventional and attributable actions to reinforce non-attributable efforts, and vice versa. Sometimes the aim is to achieve military and political objectives fast, presenting a *fait accompli* – an outcome already accomplished and presumably irreversible – before an allied response can prevent it. Note that the intrinsic ambiguity of this 'hybrid' use of measures may cause a (dangerous) divergence in perception between the source and the target on what constitutes an escalatory or de-escalatory step.

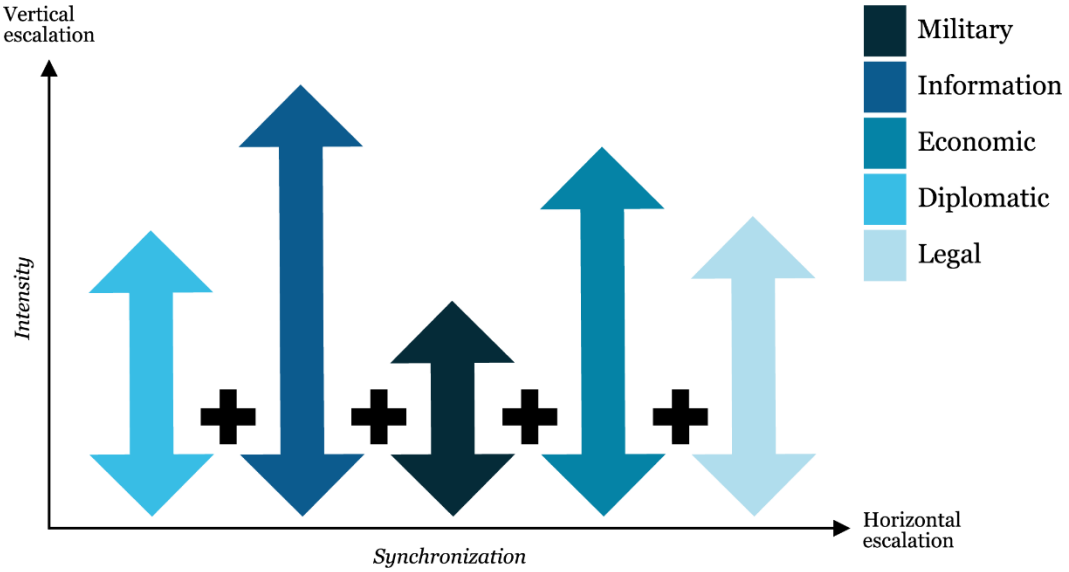

Figure 3: Combining instruments of power in hybrid conflict[5]

In principle, the escalation ladder from Figure 1 is generic in the sense that it may be applied to all DIMEL domains. However, the various levels have quite different annotations for the distinct domains and might be more applicable in some combinations than in others. Indeed, a particular low level action in one domain can have more impact than a high level action in another domain. Further note that, next to this vertical escalation ladder, moving from one DIMEL domain to another in itself may be perceived as an (horizontal) escalation step by the target, even if the initiator did not intend to escalate. In other words, the levels of escalation have no absolute value across the various instruments of power and influence. (Figure 4 depicts a nominal horizontal escalation hierarchy.)

[5] Based on Multinational Capability Development Campaign (MCDC) 2015-2016, *Countering Hybrid Warfare (CHW) Analytical Framework*, 31 October 2016

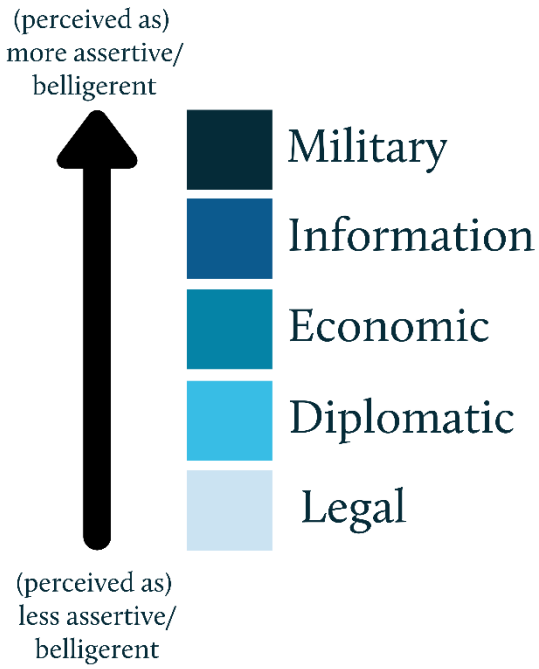

Figure 4: Intrinsic horizontal escalation hierarchy of the DIMEL domains

From Single Domain to Cross-Domain Strategies: Issues to Consider

The cross-domain character of contemporary conflict adds another layer of complexity to the portfolio of strategic options, namely the multiplicity of instruments through which the strategic efforts can be conducted. To provide guidance on how to think about the salient issues in the selection and execution of cross-domain strategies in hybrid conflicts, we have delineated five kinds of assessment that need to be conducted before, during, and after the employment of strategies in the cross-domain context.

Cost-Benefit Assessment. This type of assessment presupposes prior selection and prioritization of objectives. It is relevant to start with the assessment of benefits because these should be directly related to the objectives that are pursued. The bottom line is that no matter how great the benefits are, if they do not contribute to the relevant objectives then the strategy may be either irrelevant or outright damaging. The calculation of benefits in the cross-domain context needs to consider the potential interaction between instruments, which may enhance or degrade each other's effects. For example, the potential benefits of controlling strategies are likely to be enhanced when conducted across military, diplomatic and economic domains, because in all these forms the strategies drain away from the adversary's resources. On the other hand, coercive strategies conducted across domains may not enhance each other's potential because the adversary is likely to pay attention to the most dangerous threats and to ignore or neglect the rest of them. A similar logic applies to the assessment of costs in the cross-domain context. Controlling strategies exercised across military and economic domains are always bound to be expensive while those relying on the use of diplomacy and information may be cheaper. The cost-benefit assessment should also

consider the potential costs associated with risks attached to a particular course of action and its failure.

Cross-Domain Orchestration Assessment. Strategy needs to be implemented in practice. The cross-domain context allows for a broad spectrum of options to choose from. For small and middle powers, the international context and the position of allies and friendly nations will need to be considered since actions are typically conducted within the context of international coalitions. It is then crucial to know the priorities and means available to others because these determine the character and the extent of effort allies are willing to invest on their own behalf. Cross-domain orchestration at both the international and the national level brings with it an assortment of additional challenges. It is necessary to know who is responsible for the mobilization, coordination and employment of the diplomatic, information, cyber, economic, military and legal instruments as well as which actors possess the mandate to employ these resources to pursue objectives in unlike domains. The complexity of orchestrating cross-domain instruments are further exacerbated by the fact that responsibilities and capabilities are spread out over different government departments. It is therefore necessary to identify the mandate and the responsibilities for the use of resources in addition to the coordination mechanisms for how these means can be used.

Proportionality Assessment. The appraisal of the cross-domain strategy's proportionality in relation to the particular challenge at hand requires an assessment of that challenge. Proportionality is then a subjective metric but it is generally a function of two distinct sources – instruments and effects. Proportionality of instruments relates to the character of the domains in and through which the strategy is employed. A basic level of proportionality can be achieved by using military instruments to counter military threats and non-military instruments to counter non-military threats. It also follows that, in general, using the military instrument to counter non-military threats is likely to be disproportional. The proportionality of effects is more complicated because the latter cannot be easily categorized and, therefore, contrasted. Nonetheless, it is possible to divide effects into physical and psychological ones. Physical effects are more proportional to other physical effects while psychological effects are more proportional to psychological effects. At the same time, it is necessary to acknowledge that in the cross-domain context most instruments, most of the time, produce both physical and psychological effects. It is therefore necessary not only to assess the character of the effects but also their severity. For example, while military and economic control both produce physical effects, the former tends to be more severe than the latter, particularly in the short run. These points tie back to the escalation ladder introduced earlier, which is essential to navigate potential escalation dynamics during the conflict.

Signaling Assessment. This type of assessment pertains to the anticipation of how the adversary, as well as domestic and international audiences, are likely to perceive the actions and what psychological effects will be produced by strategic signaling. The execution of every strategy signals a message, whether that message is intended or not. The psychological effects of signaling largely depend on the cognitive processes of the respective audience and on the escalation potential of particular domains. For this reason, it is necessary to have some level of understanding of the particular belief systems and perceptions of the relevant audiences. At the same time, it is also crucial to understand that strategies conducted in and through some domains may appear less

escalatory than those conducted in other domains. Signaling will be more complicated in some domains than in others. The solution to the signaling puzzle resides in the right combination of instruments so that these enhance each other's signaling potential. For example, coercion exercised through cyber instruments could be complemented by economic or military instruments so that the adversary is less likely to misunderstand or ignore the message. In sum, the assessment of effects produced by strategic signaling rooted in a good understanding of an opponents' belief system sheds light on the potential conversion rate between the use of strategies and the psychological consequences they are likely to create.

Legal and Normative Frameworks Assessment. Here the first question is whether the domestic legal framework allows for the selection of the strategy but also whether it allows for the prolonged exercise of the strategy. It is necessary to assess which options are legal in particular domains but also across them. For example, some legal frameworks may only allow for offensive cyberattacks to target military rather than civilian infrastructure. The second question is concerned with the legitimacy of the strategy from the perspective of both international law and international norms. Additionally, it is also important to assess whether the conduct of particular strategy conveys the emergence or propagation of a new norm of behavior or whether it falls within the framework of the existing norms.

The five assessments and the types of questions that need to be asked are summarized in the table below.

	Core assessment question	Particulars
1. Effects and Success	How does the cross-domain strategy fare in the cost/ benefit assessment?	• What are the political objectives? • What are the potential benefits and costs associated with the strategy? • What are the potential sources of failure across domains? • How do we define success? • Can we measure success?
2. Proportionality	How proportional is the cross-domain strategy in relation to the threat?	• What is the character of the challenge? • Is the character of the instruments employed proportional to the character of the challenge? • Is the character of the potential effects proportional to the severity of the challenge?
3. Orchestration	How can the strategy be executed and orchestrated in the cross-domain context?	• What sort/ form of support can we expect from our allies? • What means are available across all domains? • Who has the mandate and the responsibility to mobilize and use these respective means? • What are the specific limitations and opportunities associated with the employment of the particular means? • How can these means be synergistically employed across domains?
4. Doctrinal and legal frameworks	What is the relationship of the particular cross-domain strategy to the relevant domestic and international legal and normative frameworks?	• What is the domestic and international legal framework covering the actions included in the strategy? • What international norms pertain to the exercise of the strategy? • How does the strategy shape international norms?
5. Signaling and communication	What are the likely signaling effects of the strategy?	• What are the audience's belief system and perceptions? • How escalatory is the strategy in different domains to be perceived by the adversary?

Table 2 From Single Domain to Cross-Domain: Issues to Consider

Conclusion

The framework goal of this project is to offer a menu of strategies that can be used to actively counter hybrid threats. Accordingly, five strategies can be employed simultaneously or sequentially to counter hybrid threats. These strategies are cooperation, persuasion, protection, coercion, and control. These can be exercised through and across six different domains: diplomatic, information, cyber, economic, military, and legal. The detailed overview of conceptual strategies accompanied by examples of concrete measures provided in this document offer levers for the formulation of a counter hybrid strategic posture.

The theoretical propositions need to be further developed and tested. Strategic practice may falsify some of its assumptions or it may motivate further adjustments or refinements of its constituting elements. For this purpose, insights will be refined in a simulation environment in the form of a table-top game to shed light on how the strategies work in a simulated competitive setting. The findings gained from this exercise will help refine the framework and inform the crafting of effective cross-domain strategies in the real world.

1 Introduction

This document serves as a background document to prepare a hybrid conflict game organized by TNO in collaboration with HCSS to gain a better understanding of how cross domain strategies can help in countering hybrid threats.[6]

Hybrid conflict became more salient during the 2010s and is not likely to wither away in the 2020s. The Netherlands, together with likewise partners in its network of alliances, requires a strategic posture to deal with it. The goal of this document is to lay out a menu of strategies that can be used to actively counter hybrid threats, embedded in a strategic framework that conceptualizes the range of possible strategies in a structured way. The aim of such a framework is to help in understanding both the problem space and the solution space; to offer a range of optional strategies that can be considered in countering the palette of hybrid threats; and to show how these strategies can relate to and complement one another.

Such a framework is not only relevant in the identification of appropriate response measures. It can also be used to design a strategic posture. A strategic posture refers to the set of dominant strategies that make up a state's security policy to achieve a set of objectives. A strategic posture is guided by an overarching purpose and objectives (ends) and offers general guidelines as to how to act and react (ways), thus providing guidance for the development of capabilities (means). In the case of hybrid threats, a strategic posture can:

- assist in defining and preparing the pre-requisites for counter hybrid action in terms of capabilities, legal and doctrinal frameworks, and mandate allocation;
- be instrumental in creating unity of action and synergy between counter hybrid measures by tying them together in one coherent whole;
- help in communicating to opponents and allies what are considered to be acceptable forms of hybrid behavior. It can thereby be instrumental in the development of international norms that limit hybrid threat behavior; and
- thus ultimately shape the cost calculus of an adversary which in turn can prompt changes in adversarial behavior.

Although a strategic posture represents a codification of the ends and ways, it is dynamic in nature because the evolving character of challenges requires adaptiveness. This document lays down the rationale for the strategic framework and defines and describes the strategies. It describes how these strategies can be plotted on a notional escalation ladder across the different DIMEL domains.[7] For each of the strategies, it offers illustrative examples of concrete measures that can be taken across the DIMEL Domains. It then describes a number of issues that need to be considered in the selection and execution of cross-domain strategies, which will be further examined in the hybrid cross-domain strategy game to be held in the summer of 2020 in The Hague.

[6] It will also be used for the purposes of another study conducted by the HCSS on the development of international norms to shape responsible behavior in hybrid conflict.
[7] DIMEL = Diplomatic, Informational, Military, Economic, Legal.

2 Strategic Framework to Counter Hybrid Action

2.1 Scope of the Framework: Beyond Deterrence as a Catch-All Term

The strategic response framework we present here describes and explains relationships between strategies and counter-strategies in dealing with hybrid threats, building on insights identified in the broader counter hybrid threat literature.[8] One strand of that literature predominantly focuses on the conceptual analysis and the empirical description of hybrid threats and hybrid threat behavior.[9] Another strand concerns itself more directly with the question how to counter these threats.[10]

In that second strand, alongside building stronger protections against hybrid intrusions and strengthening societal resilience, deterrence has been singled out as an important part of counter hybrid policies.[11] The rationale behind it is relatively straightforward: how to get adversaries to refrain from engaging in hybrid threat behavior that damages vital interests without having to use large scale violence. It is recognized, however, that hybrid threats are difficult to prevent through deterrence alone for an assortment of reasons. In a globally connected multipolar security environment, technological developments have contributed to the democratization of the means of violence. This, at least in some cases, favors the offensive and renders deterrence unstable.[12] Furthermore, by their very nature, hybrid actions are not always easily attributable

---

[8] See also Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone* (Santa Monica: RAND Corporation, 2019).

[9] For theoretical and conceptual treatments, see Frank G Hoffman, 'Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges', *PRISM* 7, no. 4 (November 2018): 30–47, https://doi.org/N/A; Frank G Hoffman, 'Conflict in the 21st Century: The Rise of Hybrid Wars' (Arlington: Potomac Institute for Policy Studies, December 2007). Robert Johnson, 'Hybrid War and Its Countermeasures: A Critique of the Literature', *Small Wars and Insurgencies* 29, no. 1 (December 2017): 141–63. Fridman, *Russian 'Hybrid Warfare'*; Stoker and Whiteside, 'Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking'; , For the empirical works, see Murray and Mansoor, *Hybrid Warfare*. Hall Gardner, 'Hybrid Warfare: Iranian and Russian Versions of "Little Green Men" and Contemporary Conflict' (Rome: NATO Defense College, December 2015), https://css.ethz.ch/en/services/digital-library/publications/publication.html/195396. Andrew Radin, 'Hybrid Warfare in the Baltics', Product Page (Santa Monica: RAND Corporation, 2017), https://www.rand.org/pubs/research_reports/RR1577.html.

[10] Cullen and Wegge, 'Countering Hybrid Warfare'. Michael Rühle, 'NATO's Response to Hybrid Threats' (Washington: National Institute for Public Policy, 4 November 2019), https://www.nipp.org/2019/11/04/ruhle-michael-natos-response-to-hybrid-threats/. Michael Rühle, 'Deterring Hybrid Threats: The Need for a More Rational Debate', NDC Policy Brief (Rome: NATO Defense College, 9 July 2019), http://www.ndc.nato.int/news/news.php?icode=1335. Sean Monaghan, 'Countering Hybrid Warfare', *PRISM* 8, no. 2 (2019): 82–99. Kersanskas, Vytautas. "Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats." Hybrid CoE, March 2020. https://www.hybridcoe.fi/wp-content/uploads/2020/03/Deterrence. pdf.

[11] Robert J. Vince, 'Cross-Domain Deterrence Seminar Summary Notes', Government & Nonprofit (Livermore: Center for Global Security Research, May 2015), https://www.slideshare.net/LivermoreLab/summary-notes-47797997; Cullen and Wegge, 'Countering Hybrid Warfare'. Mallory, 'New Challenges in Cross-Domain Deterrence'.UK Multinational Capability Development Campaign 2019. Stephen Flanagan J et al., *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance* (Santa Monica: RAND Corporation, 2019). Uwe Hartmann, 'The Evolution of the Hybrid Threat, and Resilience as a Countermeasure' (Zurich: Center for Security Studies, October 2017), https://css.ethz.ch/en/services/digital-library/articles/article.html/3eadb4fb-09de-4b79-93b1-af1ee4117a0d/pdf. Hybrid CoE, *Deterring Hybrid Threats: A Playbook for Practitioners* (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, 2020).

[12] Andrew F. Krepinevich, 'The Eroding Balance of Terror: The Decline of Deterrence', *Foreign Affairs*, February 2019, https://www.foreignaffairs.com/articles/2018-12-11/eroding-balance-terror.

which puts a strain on the possibility of deterrence.[13] Authors have also pointed to the overall declining payoffs associated with the manipulation of fear across a variety of domains which can be partially extrapolated to the security domain.[14] Finally, there is general consensus that our understanding of the role of psychology and perceptions has progressed to such a degree that it is necessary to broaden the framework to include influence strategies beyond deterrence alone.[15] For that reason it is argued that we need to focus on other means – both negative and positive – to dissuade but also persuade adversaries.[16] This brings us full circle back to insights already coined in the traditional deterrence literature which defines it as "a process of influencing the enemy's intentions, whatever the circumstances, violent or non-violent."[17]

Given the nature of hybrid threats, prevailing concepts of deterrence have therefore been expanded considerably. Though age-old in practice, deterrence as a modern concept, emerging in the inter-war period. For the first time in history, it was possible to harm civilians populations without first dealing with their armed forces. While not named as such, deterrence through the threat of retaliation by air bombardments was first discussed by strategic thinkers in these years. The term itself and the conceptual clarification emerged shortly after the invention of nuclear weapons. While much of the minutiae of deterrence theory weas refined and adjusted over the next four decades, the general content remained more or less the same. The notable exception was the distinction made between the original emphasis on retaliation and the newly added notion of denial. Instead of focusing on the threat of punishment, denial inverted the logic of deterrence by deploying attention to the threat of failure. This was a significant modification and the first in a string of many more to come. However, in other aspects, deterrence remained narrowly conceptualized. It was still predominantly about the use of military measures, though gradually conventional means became discussed next to the nuclear ones.[18]

The concept of deterrence has changed considerably from the end of the Cold War onward. The new security environment is characterized by the proliferation of non-state actors who pose a wide range of threats. Consequently, the character and ultimately the nature of deterrence has transformed. Inspired by the Israeli concept of deterrence, developed largely independently from the Euro-Atlantic perspective, one strand of deterrence scholarship now advocates the actual use of violence to be included in the deterrence mechanism (as opposed to mere threats).[19] Additionally, both denial and punishment have expanded far beyond their original proportions. In addition to traditional defensive measures, denial now includes resilience and offense as inherent components. Resilience is directed at dissuading hostile measures by presenting the

---

[13] Aaron Brantly, 'Back to Reality: Cross Domain Deterrence and Cyberspace' (Boston: Virginia Tech, 2018), https://vtechworks.lib.vt.edu/bitstream/handle/10919/85386/Brantly-Back2Reality-APSA-DRAFT.pdf?sequence=1&isAllowed=y.

[14] De Spiegeleire et al. 2020.

[15] Michael Mazarr et al., *What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression* (RAND Corporation, 2018), https://doi.org/10.7249/RR2451.;

[16] Stephan De Spiegeleire et al., 'Reimagining Deterrence: Towards Strategic (Dis)Suasion Design' (The Hague: The Hague Centre for Strategic Studies, March 2020).

[17] Snyder, *Deterrence and Defense*, 11.

[18] John Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1985).

[19] Thomas Rid, 'Deterrence beyond the State: The Israeli Experience', *Contemporary Security Policy* 33, no. 1 (April 2012): 124–47, https://doi.org/10.1080/13523260.2012.659593.

adversary with the futility of his attacks through recovery, whilst offense is supposed to achieve the same ends by destroying the means through which the adversary might conduct the attacks.[20] Denial has also broadened. It is now discussed, mostly in the form of resilience, across all sectors of society and far beyond the original military meaning.[21] Punishment too has acquired a revised meaning in the contemporary world. Concepts such as cumulative or punctuated deterrence were proposed to convey punishment delivered over time or in repeated instances, respectively.[22] Non-military instruments are now common tools for the pursuit of punishment through entanglement, shaming or stigmatization.[23] Others have proposed that proverbial carrots should be carried in tandem with the sticks so that deterrence may also be executed through the promises of rewards and positive incentives.[24]

In sum, the concept of deterrence now encompasses almost every conceivable strategy. On the one hand, the expanded concept offers a broad spectrum of strategies to tackle the diverse character of contemporary challenges. On the other hand, it confuses more than it illuminates. It puts a burden on deterrence responsibilities and requirements that is almost impossible to meet: "If deterrence is responsible for preventing every possible malign act an adversary might pursue, be it cutting undersea cables, orchestrating fake news campaigns, or hacking smartphones, deterrence strategies must be organized so as to prevent a nearly unending list of hostile behavior."[25] It blurs the distinctions between individual instruments of power, between different levels of analysis, and ultimately between the basic tenets of human psychology. The specific strategies and instruments of power vary widely in their effects, in reality and as perceived by different adversaries; with military means differing from all the others in their means (violence) and consequences (control). Finally, humans perceive and react differently to positive and negative stimuli. For example, due to the well-documented negativity bias, we pay much more attention to objects and events that we deem unpleasant.[26] The logic of combining all these measures under the deterrence label is not clear. It is possible that most of these measures may dissuade the adversary's hostile actions. They can, therefore, produce deterrent effects. However, determining whether this potential is perceived as threatening depends solely upon the interpretation of the adversary. By contrast, deterrence as a practice of actively using threats only relates to the concept of punishment through retaliation. It is for this reason that we chose to deal with deterrence separately from the other strategies.

---

[20] Flanagan et al., *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance*; Efraim and Shamir, '"Mowing the Grass": Israel's Strategy for Protracted Intractable Conflict'.

[21] Theo Brinkel, 'The Resilient Mind-Set and Deterrence', in *Netherlands Annual Review of Military Studies*, ed. Frans Osinga and Paul Ducheine (The Hague: Asser Press, 2017), 19–38.

[22] Doron Almog, 'Cumulative Deterrence and the War on Terrorism', *Parameters* 34, no. 4 (Winter 2004): 4–19; Uri Tor, '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence' 40, no. 1–2 (2015): 92–117; Lukas Kello, *The Virtual Weapon and International Order* (Yale: Yale University Press, 2017).

[23] Joseph S. Nye, 'Deterrence and Dissuasion in Cyberspace', *International Security* 41, no. 3 (January 2017): 44–71, https://doi.org/10.1162/ISEC_a_00266.

[24] Michael J. Mazarr, 'Understanding Deterrence', 2018, 5, https://www.rand.org/pubs/perspectives/PE295.html.

[25] 'In Defense of Deterrence | RealClearDefense', accessed 2 June 2020, https://www.realcleardefense.com/articles/2020/04/30/in_defense_of_deterrence_115237.html.

[26] Paul Rozin and Edward B. Royzman, 'Negativity Bias, Negativity Dominance, and Contagion', *Personality and Social Psychology Review* 5, no. 4 (2001): 296–320.

2.2 A Framework of Strategies

We therefore suggest a framework that does not collate all these strategies but differentiates between them. We suggest a framework consisting of five general strategies: cooperation, persuasion, protection, coercion, and control (See Table 2). Our framework explicitly draws on and extends the survey of King Mallory on different strategies in his analysis of cross domain deterrence from 2018.[27]

Strategy	Description
Cooperation	The pursuit of reciprocally beneficial policies to maximize mutual gains for both the source and the target[28]
Persuasion	The use of rewards to achieve cooperation from the target
Protection	The increase of the source's capability to withstand or absorb hostile measures
Coercion	The use of threats to prevent or change the target's behavior
Control	The use of force to limit the target's freedom of action

Table 3 A framework of strategies

Cooperation involves the coordination of mutually beneficial policies to "improve political relations".[29] Strategies of cooperation actively pursue collaborative efforts to achieve shared goals on the basis of mutual interest. It can also entail working actively to create shared interests. The purpose of cooperation is to maximize mutual gains and to avoid reciprocal losses. Cooperation can manifest itself in various forms of entanglement, conciliation and accommodation. Entanglement denotes the development of interdependencies which make hostile measures costly to the source and the target alike.[30] Examples typically take the form of mutual dependencies, usually economic or supply-chain, whose disruption would reciprocally harm both actors and thus disincentivize destabilizing actions. Conciliation refers to "removing key obstacles to reaching an agreement, without agreeing to a major part of the other side's demands."[31] This is a convention of integrative bargaining, a mode of negotiation which seeks a win-win solution rather than win-lose zero-sum distributive bargaining. Finally, accommodation refers to giving in to "substantial but relatively painless portion[s] of the other sides demands to achieve agreement".[32] Unlike conciliation, which entails no loss to either side, this involves minor concessions from one side, although they may be communicated as substantial concessions to the target. Historical precedents include the US-Soviet missile exchange at the height of the Cuban Missile Crisis, by which the US agreed to withdraw missiles from Turkey which were already slated for removal, in

[27] King Mallory, 'New Challenges in Cross-Domain Deterrence', (Santa Monica: RAND Corporation, 2018), https://www.rand.org/pubs/perspectives/PE259.html.
[28] In the remainder, 'source' refers to the actor taking a measure and 'target' to the intended recipient or audience of the measure. Of course, in an action-reaction sequences, measures provoke countermeasures in which 'source' and 'target' are reversed.
[29] Charles L. Glaser, *Rational Theory of International Politics* (Princeton: Princeton University Press, 2010), 51.
[30] Nye, 'Deterrence and Dissuasion in Cyberspace', 58.
[31] Mallory, 'New Challenges in Cross-Domain Deterrence', 2.
[32] Mallory 2018, 2.

return for Soviet withdrawal from Cuba.[33] There is a thin line between accommodating and sacrificing one's interests in order to appease the other side.[34] The crucial caveat associated with a strategy of cooperation is that it requires that the other party recognizes these overtures and acts in good faith. Absent this reciprocal good faith, that party can exploit a cooperative strategy to achieve its own objectives, or revert to confrontational distributive bargaining. Given these characteristics, cooperation can enhance protective and persuasive strategies. It may stack with coercion but is unlikely to work well alongside control.[35]

Persuasion uses promises of positive incentives, or rewards, to gain cooperation from the other side to persuade an opponent to engage in certain behavior.[36] The purpose of persuasion is to alter the target's behavior. Successful persuasion leads to win-gain scenarios. Persuasion can come in material and immaterial forms. Material forms of persuasion include economic inducements or other tangible rewards.[37] Immaterial forms include the prospects of status, prestige, good relations or credible reassurances about the other's security.[38] Persuasion also requires goodwill on the part of the target. This can be alleviated by combining persuasion with some form of coercion in order to provide the proverbial stick to the carrot.[39] Persuasion does not work well alongside control strategies because it loses much of its credibility when unilateral violence is introduced into the equation; however, it can certainly work well alongside cooperation, to create better terms for cooperation, as well as with coercion, to add carrots to the proverbial stick. The principal element of persuasion is to provide an incentivizing alternative for a target rather than continued confrontation. As such, it requires a pause or reversal of escalatory actions, and effective communication to convey overtures by which a target can reciprocate without being seen to lose legitimacy or capitulate.

---

[33] Churchman, David, *Negotiation: Process, Tactics, Theory*, 1995.

[34] Despite these sacrifices, appeasement can still work as an effective cooperative strategy. See for example Stephen R. Rock, *Appeasement in International Politics* (Lexington: University Press of Kentucky, 2000).

[35] For one theorized way in which cooperation, persuasion, protection and coercion can work alongside each other, see Morris et al., *Gaining Competitive Advantage in the Gray Zone*, 136–54.

[36] For a more detailed explanation for the logic behind persuasion, see David J. Singer, 'Inter-Nation Influence: A Formal Model', *The American Political Science Review* 57, no. 2 (June 1963): 426–27, https://doi.org/10.2307/1952832.

[37] For a detailed overview of how economic inducements work in practice, see Patricia A. Davis, *The Art of Economic Persuasion: Positive Incentives and German Economic Diplomacy Kindle Edition* (Ann Arbor: University of Michigan Press, 1999). and William Long, *Economic Incentives and Bilateral Cooperation* (Ann Arbor: University of Michigan Press, 1996).

[38] Herbert C. Kelman, 'Social-Psychological Dimensions of International Conflict', in *Peacemaking in International Conflict: Methods and Techniques*, ed. William Zartman, 2nd ed. (Washington: United States Institute of Peace, 2007), 72–78..

[39] Alexander George and Graham Stuart, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War* (Washington: United States Institute of Peace, 1992), 10–11..

Protection involves strategies aimed at increasing security by reinforcing one's ability to defend against hostile measures or withstand the impact of hostile measures. A successful conduct of protective strategies typically results in win – zero scenarios. The two basic forms of protection are resilience and defense. Resilience defines the "ability to absorb the direct impact of hostile activity without suffering any long-lasting impact."[40] Defense involves being able to deny the target the ability to harm you from the outset, thereby "reducing [y]our own prospective costs and risks."[41] The function of defense is therefore to thwart attacks, while the function of resilience is to mitigate its consequences. Both resilience and defense can be conducted across all sectors and domains. The main purpose of both resilience and defense is to deal with the actual hostile measures. Yet, if they are strong, they can also help to dissuade a target from carrying out hostile measures because the target will not yield expected benefits.[42] This gives protective strategies the potential to enhance deterrence methods. For all these reasons, both forms of protection need to be constantly updated to keep pace with the most recent character of the threats they are supposed to counter.

Coercion, in contrast to the reward-centric methodology of cooperation and persuasion, conveys persuasion to adversaries via negative means.[43] It denotes an activity that compels another actor "to do something it does not want to do."[44] The purpose of coercion is to either prevent or alter the target's behavior. Accordingly, coercion comes in the form of deterrence and compellence. Deterrence refers to the use of threats to dissuade the target from taking a particular action, of which many historical examples exist. Comparatively, compellence entails the use of threats (either directly or through implied means), to convince the target to take a particular action.[45] Successful employment of coercive strategies typically results in win-lose scenarios. Furthermore, both coercive strategies may be employed across all domains, either through overt military means or through leveraging diplomatic or economic channels.[46] Examples span the range of sanctions regimes, bilateral diplomacy, and the use of cyber and hybrid tools, as the use of explicit military tools of coercion has been reduced by (most) actors in modern times. Coercive strategies can also be conducted by threats of shaming or stigmatization.[47] The main currency of coercion is threats of retaliation (or

---

[40] See Tim Sweijs and Samuel Zilincik, The Essence of Cross Domain Deterrence, in *Deterrence* in the 21st Century—Insights from Theory and Practice. Editors: *Osinga*, Frans, *Sweijs*, Tim (Eds.), 2020 (Asser-Springer.

[41] Snyder, *Deterrence and Defense*, 3.

[42] For the dissuasive effects of defense, see Colin S. Gray, 'Deterrence and Regional Conflict: Hopes, Fallacies, and "Fixes"', *Comparative Strategy* 17, no. 1 (1998): 58–59, https://doi.org/10.1080/01495939808403131., for resilience see Hartmann, 'The Evolution of the Hybrid Threat, and Resilience as a Countermeasure'.

[43] For a beginner friendly explanation of the coercion theory, see Tami D. Biddle, 'Coercion Theory: A Basic Introduction for Practitioners', *Texas National Security Review* 3, no. 2 (Spring 2020), https://tnsr.org/2020/02/coercion-theory-a-basic-introduction-for-practitioners/.

[44] Robert J. Art and Kelly M. Greenhill, 'Coercion: An Analytical Overview', in *Coercion: The Power to Hurt in International Politics*, ed. Kelly M. Greenhill and Peter Krause, 1 edition (New York, NY: Oxford University Press, 2018), 4.

[45] Thomas C. Schelling, *Arms and Influence*, 2nd ed. (New Haven: Yale University Press, 2008), 69–71.

[46] For an introduction to the topic, see Dmitry Adamsky, 'Cross-Domain Coercion: The Current Russian Art of Strategy' (Security Studies Center, 2015), http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf; Jon R Lindsay and Erik Gartzke, 'Introduction: Cross-Domain Deterrence, From Practice to Theory', in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, ed. Erik A. Gartzke and Jon R. Lindsay (Oxford: Oxford University Press, 2019), 1–26.

[47] John D'Arcy and Tejaswini Herath, 'A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings', *European Journal of Information Systems* 20, no. 1 (June 2011): 649–51, https://doi.org/10.1057/ejis.2011.23.

punishment) through words or actions.[48] Unlike protective strategies, coercive strategies target specific adversaries for specific ends.[49] This implies that threats need to be tailored to the character of the target and the intended change in behavior. Failure to do so may lead to miscommunication, provocation and escalation. Potential failures of coercion can be redeemed through protective or controlling strategies. This implies that coercive efforts do not have to be aimed at all hostile measures but only at those which may pose a serious challenge for one's protective or control strategies. Therefore, the conduct of coercive efforts needs to be rooted in a clear understanding of one's vulnerabilities and of the character of the hostile measures, as well as a detailed understanding of the desired change in behavior one wishes to induce.

Control conveys "the purposive use of [..] force to restrict another's strategic choices".[50] The purpose of control is to limit the target's freedom of action.[51] Consequently, successful exercise of control typically leads to win-defeat scenarios. The main currency of control strategies is the offensive use of force. Control strategies involve prevention or preemption. Prevention involves the use of active measures that degrade the target's "capability to pose a threat before that threat has become imminent," such as Israeli surgical air strike on Iraqi nuclear reactor under construction in 1981.[52] Preemption conveys the use of force to eliminate immediate threats, such as when Israel attacked Egypt and started the Six Day War in 1967.[53] Strategies of control are aimed at specific adversaries. The major risk of control is that while degrading the target's capabilities, it increases rather than decreases the target's willingness to implement hostile measures in response to the attack. In other words, control may as much provoke attacks as it can prevent them. For this reason, it is beneficial only as a last option when all other strategies are likely to fail.

These five strategies can be used simultaneously or sequentially. In both cases, strategies should be used carefully to rectify each other's deficiencies and to enhance their potential. Some strategies, such as cooperation and protection, always amplify each other's potential. Other strategies, such as control and persuasion, will undermine each other if used in tandem. All strategies contain some limitations and risk of failure, and therefore no single element may constitute a singular means of ensuring security.

---

[48] Janice Gross Stein, 'Threat Perception in International Relations', in *The Oxford Handbook of Political Psychology*, 2nd ed. (Oxford: Oxford University Press, 2013), 364–65.
[49] John Baylis, 'The Concept of "Tailored Deterrence" in the "Second Nuclear Age"', *St Antony's International Review* 4, no. 2 (February 2009): 8–23.
[50] Lawrence Freedman, *Deterrence* (Cambridge: Polity Press, 2004), 26.. Freedman talks of armed force: in this context it can be used more generally.
[51] Lukas Milevski, 'Revisiting J.C. Wylie's Dichotomy of Strategy: The Effects of Sequential and Cumulative Patterns of Operations', *Journal of Strategic Studies* 35, no. 2 (January 2012): 226–28, https://doi.org/10.1080/01402390.2011.563919.
[52] Mallory, 'New Challenges in Cross-Domain Deterrence', 3.
[53] Moshe Gat (2005) Nasser and the Six Day War, 5 June 1967: A Premeditated Strategy or An Inexorable Drift to War?, Israel Affairs, 11:4, 608-635, DOI: 10.1080/13537120500233714

2.3 Vertical Escalation: Five Levels on the Escalation Ladder

Again building on and extending King Mallory's work from 2018 on cross domain deterrence, the five strategies can be plotted on an escalation ladder, a spectrum from the least escalatory to most escalatory measures (see Figure 5). Escalation refers to "an increase in the intensity or scope of conflict that crosses threshold(s) considered significant by one or more of the participants."[54] The escalation ladder represents a metaphor in crisis management in which actors can take steps to manage the intensity of the conflict, either through the escalation, de-escalation or a combination of the two via different channels in order to communicate with an adversary.[55]

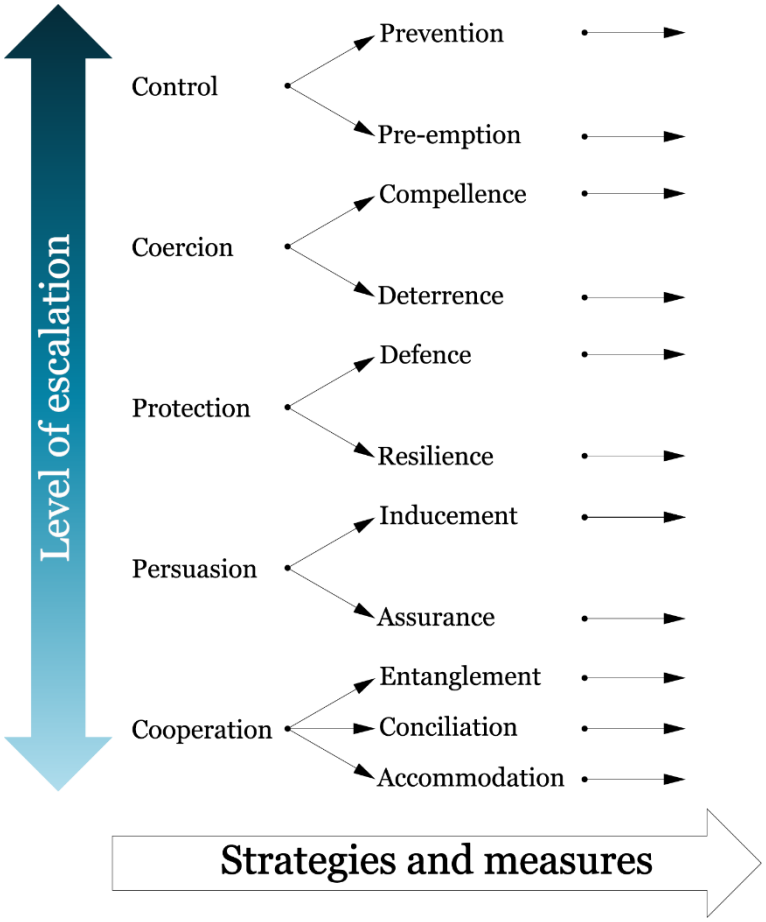

Figure 5: Strategies and an escalation ladder[56]

The least escalatory strategy is cooperation, because it is reciprocal and therefore avoids conveying aggressive behavior toward the other side. Persuasion is more escalatory than cooperation because it operates upon unilateral action conducted toward the target. The next level is protection, which is more escalatory than persuasion because it conveys the singular pursuit of one's own interest without regard for the interests of

[54] Morgan 2008, 8.

[55] The notion of an escalation ladder was coined by Herman Kahn in the early days of the Cold War to guide thinking about crisis management. Herman Kahn, *On Escalation: Metaphors and Scenarios* (Santa Barbara: Praeger, 1965).

[56] The visual is an adaptation and extension of the visual developed by King Mallory, see King Mallory, 'New Challenges in Cross-Domain Deterrence', (Santa Monica: RAND Corporation, 2018), https://www.rand.org/pubs/perspectives/PE259.html.

the other side. Coercion exerts forceful pressure towards the opponent to alter his behavior, even if this potentially hurts one's own interests. Finally, control is the most escalatory strategy because it conveys the full-fledged physical imposition of one's intent upon the target.

The idea of an escalation ladder remains as relevant today as ever. It is possible to use the outlined strategies to climb up and down the ladder. It is worth noting that all strategies can be used for escalatory and de-escalatory purposes *except* cooperation, which by definition leads to de-escalation. Whilst the capacity of control or coercion to de-escalate may seem paradoxical, it is inherent to the overall communication methods between adversaries. These strategies can decrease the target's overall will to fight by threats or by the destruction of their capabilities. It is therefore possible to use control to deescalate as much as it is possible to use protection to escalate. This also implies that strategies should be employed carefully to augment each other's (de)escalatory potential rather than hinder, or in the case of using control and persuasion strategies simultaneously, undermine each other. If one seeks escalation, then it does not make sense to use cooperation alongside coercion and vice versa. The common denominator between strategies must be recognized in their utilization across domains.

2.4 Horizontal Escalation: the DIMEL Domains

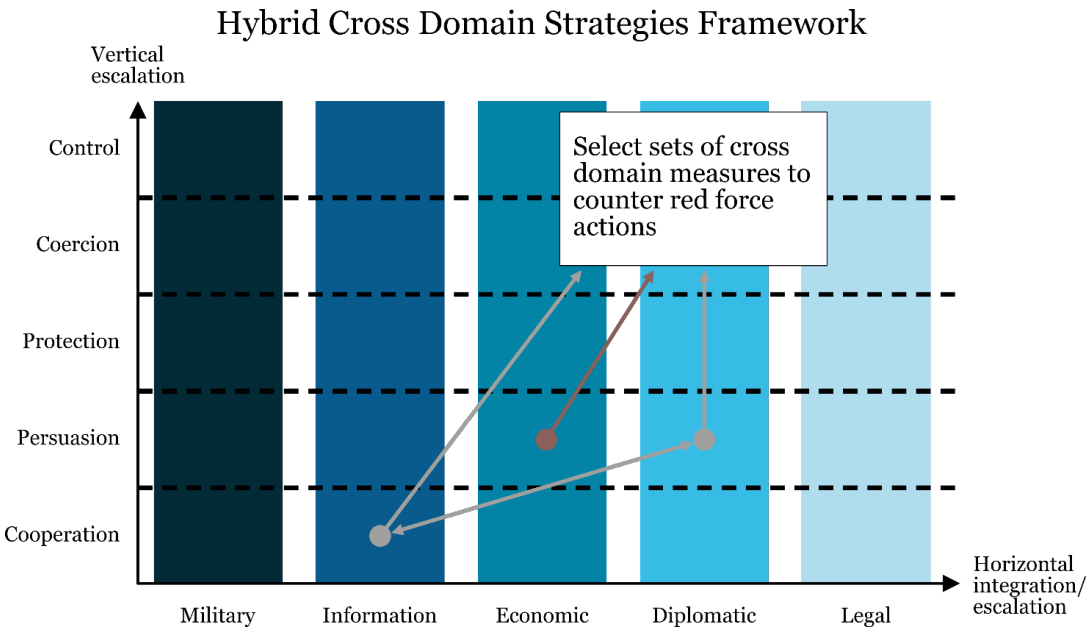

Figure 6: Cross-domain escalation

One can escalate vertically as well as horizontally (see Figure 6).[57] For this, we use the well-known DIMEL categorization of instruments of state power, distinguishing between the Diplomatic, Information, Military, Economic and Legal domains. Vertical actions convey escalation within the same domain. For example, if hostile measures revolve around cyber espionage, a vertically escalating response may include acts of

[57] For the original work, see Kahn, *On Escalation: Metaphors and Scenarios*. For adaptation to the cross domain context, see Tim Sweijs and Samuel Zilincik, 'Cross Domain Deterrence and Hybrid Conflict' (The Hague Centre for Strategic Studies, 2019), 14, https://hcss.nl/sites/default/files/files/reports/Cross%20Domain%20Deterrence%20-%20Final.pdf.

cyber sabotage. In contrast, to escalate horizontally means to broaden the scope of efforts beyond the present DIMEL domain and associated category of measures. For instance, diplomatic and economic sanctions can be used in response to military aggression, as the West did in the aftermath of the Russian annexation of Crimea. Going one level deeper, horizontal escalation can also take place within various military domains. Israel, for instance, used airstrikes against Hamas in the spring of 2019 in retaliation for a series of cyberattacks, utilizing a kinetic countermeasure to a cyber threat.[58]

In hybrid conflicts, actors not only switch between domains but combine the different power instruments while varying the level of intensity per domain (see Figure 7) . By doing so, hybrid actors typically move up and down the escalation ladder in what is called the 'grey zone' between war and peace, while avoiding the threshold that would traditionally lead to open (military) conflict. In addition, hybrid tactics leverage conventional and attributable actions to reinforce non-attributable efforts, and vice versa (the textbox below describes Russia's hybrid activities during the Crimea Crisis). Sometimes the aim is to achieve military and political objectives fast, presenting a fait accompli – an outcome already accomplished and presumably irreversible – before an allied response can prevent it. Note that the intrinsic ambiguity of this 'hybrid' use of measures may cause a (dangerous) divergence in perception between the source and the target on what constitutes an escalatory or de-escalatory step.

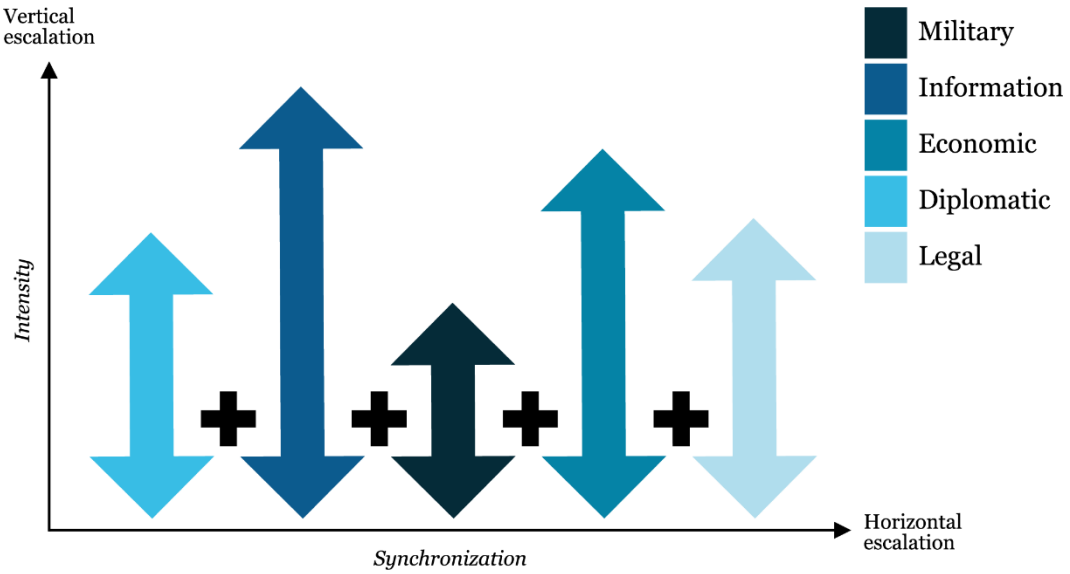

Figure 7: Combining instruments of power in hybrid conflict[59]

[58] Erica D. Borghard and Jacquelyn Schneider, 'Israel Responded to a Hamas Cyberattack with an Airstrike. That's Not Such a Big Deal.', *Washington Post*, 9 May 2019, https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/.

[59] Based on Multinational Capability Development Campaign (MCDC) 2015-2016, *Countering Hybrid Warfare (CHW) Analytical Framework*, 31 October 2016.

Russia's use of DIMEL instruments in Crimea

Diplomatic:

- Consistently denying Moscow's involvement in the conflict and framing Russia as an interested power rather than a party to the conflict.

Informational:

- Denying the involvement of Russian troops.
- Exaggerating Russia's military prowess and success.
- Using Internet trolls to spread Russia's narrative and denounce Ukraine's leadership.
- Using Russian-language broadcasting tools for propaganda and psychological operations.

Military:

- Conducting snap exercises.
- Employing 'little green men', military personnel without insignia.
- Executing unannounced flights in NATO airspace.
- Threatening the use of nuclear weapons.

Economic:

- Enforcing trade embargoes on the gas supply to Ukraine and Crimea.
- Targeting the Russian diaspora, making promises about pension money in Crimea.

Legal:

- Defending the legitimacy of the referendum on separation of Crimea from Ukraine, taking the (supposedly) equivalent unilateral declaration of independence by Kosovo in the 1990's, supported by many Western states, as a precedent.

Box 1 Russia's use of DIMEL instruments in Crimea

In principle, the escalation ladder from §0 is generic in the sense that it may be applied to all DIMEL domains. However, the various levels have quite different annotations for the distinct domains and might be more applicable in some combinations than in others. Indeed, a particular 'low level' action in one domain can have more impact than a 'high level' action in another domain (concrete examples will be offered in Chapters 3 and 4).

Further note that, next to this vertical escalation ladder, moving from one DIMEL domain to another in itself may be perceived as an (horizontal) escalation step by the target, even if the initiator did not intend to escalate. In other words, the levels of escalation have no absolute value across the various instruments of power and influence. (Figure 8 depicts a nominal 'horizontal' escalation hierarchy.)

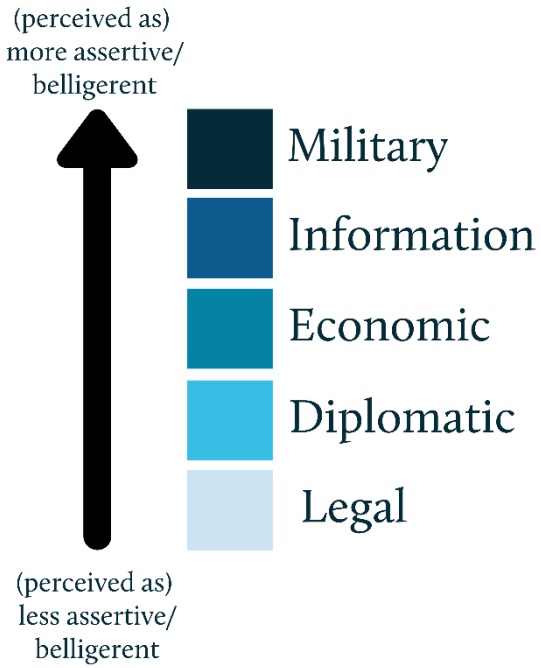

Figure 8: Intrinsic 'horizontal' escalation hierarchy of the DIMEL domain

3 Concrete Measures for Strategies In DIMEL domains

In this chapter, we elaborate on the framework introduced in the previous chapter through examples within a single DIMEL domain before we come to more complex cross- and multi-domain measures in Chapter 0. This serves to develop a better understanding of how the various levels of intensity and escalation play out across different domains. We define 'domain' as a pathway that differs from other means in terms of its political utility.[60] Accordingly, we discuss the five strategies in diplomatic, information, military, economic, and legal domains.

3.1 Diplomatic Domain

The diplomatic domain enables the use of negotiation for the purposes of policy. It can be conducted on the individual level (by diplomats) as well as on the societal level (by whole states). While diplomacy is as old as statecraft itself, modern communication technologies allow for negotiations to take place faster and more often. This change in the character of means implies that diplomacy in the contemporary world is a dynamic and potent instrument of states' power.

Strategy	Type	Generic diplomatic measures
Control	Preemption	Expelling diplomats; restricting adversaries access to international diplomatic forums, thereby limiting their diplomatic options.
	Prevention	Surrounding the adversary with a circle of hostile/neutral states (diplomatic isolation) to make it hard to launch serious hostile measures. For example, this can take the form of the integration of states in a diplomatic alliance such as the accession of former Warsaw-pact states as NATO members in 1999 and 2004.[61]
Coercion	Force	Threatening diplomatic isolation in order to change the adversary's current behavior. For example, the West has threatened Russia with diplomatic isolation repeatedly to terminate the latter's conduct of war in Ukraine.[62] Alternatively, threats of non-compliance or withdrawing from an organization, cutting off assistance, or undermining an opponent's legitimacy if it attempts to deviate from one's interests. Examples include the Turkey-EU Migration Deal: Turkey's utilization of migratory flow and diplomatic pressure to extort money from the EU in return for preventing border crossings;[63] and the US threatening the ICC court with sanctions if the court continues its prosecution of US soldiers for war crimes in Afghanistan.[64]

[60] This definition is inspired by Lindsay and Gartzke, 'Introduction: Cross-Domain Deterrence, From Practice to Theory', 16.
[61] 'A Short History of NATO', *NATO* (blog), accessed 13 May 2020, https://www.nato.int/cps/en/natohq/declassified_139339.htm.
[62] Charlotte McDonald-Gibson, 'Ukraine Crisis: EU Threatens Russia with New Economic Sanctions', *The Independent*, 27 January 2015, https://www.independent.co.uk/news/world/europe/ukraine-crisis-eu-threatens-russia-with-new-economic-sanctions-10006736.html.
[63] Reuters, 'Turkey Shouldn't Coerce Greece, Europe over Migrants: Greek PM', *Reuters*, 8 September 2019, https://www.reuters.com/article/us-greece-pm-policy-turkey/turkey-shouldnt-coerce-greece-europe-over-migrants-greek-pm-idUSKCN1VT0DB.
[64] BBC, 'John Bolton Threatens ICC with US Sanctions', *BBC*, 11 September 2018, https://www.bbc.com/news/world-us-canada-45474864.

	Deterrence	Threatening diplomatic isolation in order to maintain the adversary's current behavior. For example, a collective defense based upon diplomatic alliances. Example: NATO Article 5. Collective Defense, based upon diplomacy.[65]
Protection	Defense	Development of defensive coalitions. Example: foundation of NATO in 1949 and as well as its continual expansion during and after the Cold War.[66]
	Resilience	Utilizing public diplomacy and soft power (i.e. the use of celebrities from one's own country or its reputation) to act as representatives to bolster diplomatic resilience domestically and internationally. Example: The Hague's use of its reputation as the international center of justice to mobilize diplomatic support for certain interests; Ireland's use of famous musicians (i.e. U2) to act as informal ambassadors – most recently in the purchasing of PPE.[67]
Persuasion	Inducement	Utilizing economic incentives for diplomatic means, especially as an alternative to one's offered by an adversary. Example: China offering loans without the human rights obligations typical of the US/EU/IMF schemes. Whilst ostensibly an economic tool, this generates diplomatic inducement as it ties the recipient into China's sphere of influence. Alternatively, promising or offering incentives, such as an invitation to the alliance, in order to change adversaries intentions via their interests. For example, the many EU/NATO offers of membership to the countries in the Eastern and Southern Europe.
	Assurance	Overtures to a current or former adversary that one does not intend to encroach on their territory. Alternatively, promising or creating peacetime coalitions, dissolutions of wartime alliances and greater cooperation between the formal rivals. Example: allowing Russian observers to NATO wargame simulations, to reassure and communicate that the Alliance is playing by the rule and that there is nothing to worry about.[68]
Cooperation	Entanglement	Developing shared norms, treaties and taboos; ideally within multilateral bodies that encourage interdependency and discourage deviant action. Tying diplomatic channels to economic incentives via public-private partnerships. Through this, private companies may act simultaneously as second-order diplomatic actors, and as mechanisms of entanglement (i.e. and adversary may expel one's diplomat, but risks losing the associate private sector presence of that country companies).
	Conciliation	Inviting third parties to mediate in contested issues.
	Accommodation	Compromising with the diplomatic demands of others.

Table 4 Diplomatic measures

[65] NATO, 'Collective Defence - Article 5' (North Atlantic Treaty Organization, 2019), https://www.nato.int/cps/en/natohq/topics_110496.htm.
[66] 'A Short History of NATO'.
[67] Greg Williams, 'An Irish Entrepreneur and Bono Are Fixing the PPE Crisis', *Wired*, 16 April 2020, https://www.wired.co.uk/article/ppe-shortage.
[68] NATO, 'International Observers Visit Exercise Trident Juncture 2018', *NATO* (blog), 1 November 2018, https://www.nato.int/cps/en/natohq/news_160033.htm.

3.2 Information Domain

The information domain enables the use of information for the purposes of policy. Modern information systems and networks closely connect people and institutions within societies and across societies globally. The contemporary information environment presents aggravated asymmetries between offense and defense, as the attack surface of relatively open societies is more vulnerable to aggressive state and non-state actors. Within the information domain, we distinguish cyber and non-cyber means, as the former is substantial and distinct enough within the overarching label of hybrid conflict to merit a separate table. As such, the next section primarily deals with tools of information warfare, election meddling and other novel methods of control and deterrence collectively employed, primarily, through the vector of the information domain.

3.2.1 Information Content

Strategy	Type	Generic information (content) measures
Control	Pre-emption	The use of information warfare to **disorient** the adversary before the latter launches its attacks. This may include deception (the feeding of enemy with false information) to prevent/redirect the manifestation of a potential attack. **Meddling in foreign elections and politics**, influencing a political outcome and destabilizing democracy and rule of law. While this might not have previously been considered the height of escalation within the information domain, the political fallout of the 2016 Russian interference has prioritized electoral systems as critical infrastructure, placing it at the forefront of escalating measures. Example: Russia's interference in US elections in 2016, which involved the use of spear-phishing and leaked internal documents from the Democratic National Convention to discredit the Clinton campaign.[69] Similar incursions happened in European elections (with France as a notable actor in counteracting this measure; discussed further below).[70] Alternatively, this can involve the **acquisition of the target's national media** (newspaper, TV, radio), thereby enabling the spreading of attacker's narratives.
	Prevention	Use of fake news and trolls means to undermine the target prior to direct confrontation or to avoid repercussions from one's own actions (denial). **Large-scale information/ propaganda campaigns** targeted at **specific** population groups or opposition parties, with the aim to stir up intrastate polarization, protest, uprising and/or overthrow regimes/leaderships. This is used to sow discord within a target and limit its ability to pose a threat to the attacker, typically as a preventative measure.

[69] Protecting Europe against hybrid threats, Gustav Gressel, European Council on Foreign Relations pages, 25 June 2019

[70] Understanding Russian "Hybrid Warfare" And What Can Be Done About It, Christopher S. Chivvis, RAND, 2017: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

		Example: Russian disinformation campaign following its shooting down of MH-17 above Ukraine. Although occurring after-the-fact, the Kremlin's rapid rollout of a disinformation campaign *prevented* it from suffering the domestic and international political consequences of its actions.
Coercion	Compellence	Threatening the use of information warfare to change the adversary's policy. This may include the threats of propaganda, disinformation or of **revealing sensitive information** about the adversary's misbehavior to incite domestic unrest. **Social Manipulation**: sustained campaigns of information warfare aimed at a specifically favorable change of behavior (i.e. the lifting of sanctions) within a target's information sphere. Example: sustained Russian misinformation campaigns in Estonia, Latvia and Lithuania aimed at sowing discontent with the EU/NATO and inciting ethnic Russians within each country towards disaffection. Russian ownership of tracts of the Baltic media (i.e. The First Baltic Channel (PBK))[71], its state-funded channels outperform native outlets, especially amongst ethnic Russians, and often receive payment in return for boosting the profile of Russian-friendly Baltic politicians. The result is a contested information space, wherein the Kremlin-backed outlets have more resources.[72] **Naming and shaming; denying accreditation** in order to raise attention to an actor and impose a change in behavior. Example: European/American attribution of various disinformation campaigns arising from Russia/China. The most prominent example was French President Macron. During his election he periodically banned the presence of RT/Sputnik from reporting on his campaign in response to Russia's hacking of his campaign email servers. Additionally, propaganda outlets can be **denied accreditation** by the defender in order to challenge their legitimacy in the public view.[73] However, it is important that this is done through apolitical and independent administrators to avoid blowback and polarizations (i.e. French approach to challenging Russian IW vs. US approach; the latter became domestically politicized). The threat of black-listing persons from entering one's country; diplomatic expulsion; asset freezes or incarceration. Example: Chinese internment of two Canadian citizens in retaliation for Canada's arrest of Huawei executive.[74]
	Deterrence	Threatening retaliation through information warfare so as to discourage changes in an adversary's policy. Options include counterintelligence across human and system intelligence to gather information on adversaries'

[71] The Unknown Oligarch, Inga Springe, Sallija Benfelde, Miks Salu, The Baltic Times, 25 April 2012, https://www.baltictimes.com/news/articles/31078/
[72] Russian Information Warfare in the Baltic States – Resources and Aims, Aleksander Król, Warsaw Institute, 20 July 2017, https://warsawinstitute.org/russian-information-warfare-baltic-states-resources-aims/
[73] The "Macron Leaks" Operation: A Post-Mortem, Jean-Baptiste Jeangéne Vilmer, 2017, http://www.jbjv.com/-The-Macron-Leaks-Operation-A-Post-.html
[74] Canadians Detained in China After Huawei Arrest Have Now Spent a Year in Custody, Anna Fifield and Jeanne Whalen, Washington Post: https://www.washingtonpost.com/world/canadians-detained-in-china-after-huawei-arrest-have-now-spent-a-year-in-custody/2019/12/10/3a55cd4c-1af0-11ea-977a-15a6710ed6da_story.html

		capabilities and information operations, ideally communicated to the adversary with the threat of retaliatory cost imposition or **attribution**. Example: the NL government publishing the identities of the Russian GRU operatives suspected of hacking into the OPCW. This attribution measure in the public domain triggered a cascade by which over a dozen additional GRU operatives were publicly identified, imposing significant costs upon Russia and deterring future similar action.[75] **Counterintelligence**: detecting, monitoring and foiling the target's attempts to gather intelligence on one's assets (military, diplomatic, economic, information) by using human intelligence and signals and electronic intelligence. Apart from the UK and France, none of the other EU nations has the requisite legal framework and capabilities to conduct counterintelligence in all spheres. The question arises whether counterintelligence is at a low or high escalation level. One could argue that it is a basic measure, although when a counterintel operation is unmasked the measure could quickly go up on the escalation ladder.
Protection	Defense	Identifying and challenging malign actors in the information space; this encompasses **Fact-checking** of the adversary and challenging the information itself, either with a counter-narrative or removing it altogether. This may be supplemented by collaboration with media outlets to comprehensively challenge the spread of fake news. The most common way for states to counter information warfare is through **strategic communication** and bolstering of national media infrastructure; collective action in addressing IW threats between states. Examples: joint EU initiatives working together to combat Russian disinformation (EU vs Disinfo initiative). Additionally, the EU counter-radicalization campaign focused on online jihadist material (Civil Society Empowerment Programme).[76] US counter-narratives to ISIS propaganda on social media platforms to curtail its online influence upon domestic US audiences; the *Think Again, Turn Away*.[77] Partnership with information actors to ensure a level of integrity and mitigate the actions of malign actors; this may involve intergovernmental, private or institutional sector. Cooperate/ request (or probably this could be part of an international agreement) with internet giants like Google and Facebook **not to run political adverts at all**. Examples are Facebook during the Nigerian elections in 2019[78] and Google during Canada's elections in

[75] 305 Registrations May Point to Massive GRU Security Breach, Bellingcat, 04 October 2018: https://www.bellingcat.com/news/2018/10/04/305-car-registrations-may-point-massive-gru-security-breach/comment-page-5/

[76] EU vs Disinfo, 13 May 2020: https://euvsdisinfo.eu/

[77] Here to Stay and Growing: Combating ISIS Propaganda Networks, Alberto M. Fernandez, Brookings Institute, October 2015: https://www.brookings.edu/wp-content/uploads/2016/06/IS-Propaganda_Web_English.pdf

[78] https://www.reuters.com/article/us-facebook-election-exclusive/ exclusive-facebook-brings-stricter-ads-rules-to-countries-with-big-2019-votes-idUSKCN1PA0BT

		2019.[79] US/ European states have regularly collaborated with social media platforms to remove spam/ bot accounts propagating fake news. Despite initial reluctance to cooperate, Facebook and Twitter have increasingly accommodated governments, viewing the threat of IW as a mutual interest.
	Resilience	Improvements to **digital literacy/ critical thinking** to mitigate the effects of fake news/ IW upon the populace. Digital literacy initiatives, and especially mediating the media climate of tabloid outlets to increase critical thinking and thereby contest the information space from an adversary IW campaigns. This may be conducted in partnership with media outlets, or through top-down regulation, to comprehensively challenge the spread of fake news. Adopting alternative information means to mitigate one's own vulnerability (i.e. analogue voting). Example: Post-2016 US elections have increasingly looked to paper ballot/analogue elections to mitigate the risk of electoral tampering. Whilst this does not reduce the damage posed by disinformation campaigns it does prevent direct meddling in the apparatus of the election.[80]
Persuasion	Inducement	Accommodating adversary propaganda outlets into one's own territory, ideally with the stipulation that they do not engage in overt disinformation. Example: European states allowing mainstream Russian outlets (RT/Sputnik) to operate within their information spheres, on the condition that they do not aggressively pursue disinformation tactics.
	Assurance	Promises to destroy sensitive information acquired to discredit the adversary.
Cooperation	Entanglement	Supporting media presence and reporting of journalists from the target's media outlets; transparency of information sphere. **Support for independent media:** Often information warfare campaigns are most successful in weak/poorly developed media landscapes, which cannot gather the same resources to challenge a state-backed misinformation campaign. Therefore, many actors in IW hot sports are being encouraged to support independent media as a means of challenging and raising the costs for a potential attacker.
	Conciliation	-
	Accommodation	-

Table 5 Information (content) measures

[79] https://www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new/

[80] Christian Buckler, In a Bid For Better Security, Elections are Going Analog, 3 December 2019: https://www.marketplace.org/2019/12/03/in-a-bid-for-better-security-elections-are-going-analog/

3.2.2 Information Infrastructure (Cyber Domain)

The growing prominence of cyber as a domain continues to applications of traditional deterrence, given its novel asymmetries of ambiguity and relatively inexpensive offense, and expensive and rarely effective defense. Nevertheless, recent trends indicate a growing body of credible methods of cyber defense which, alongside proactive measures, allow for the application of our escalation model. The below table deals directly with instances of cyber-attack, dispensing with broader components of hybrid warfare within the information domain which are addressed in the previous table.

Strategy	Type	Examples of cyber measures (generic and concrete examples)
Control	Pre-emption	The use of offensive cyber-attacks directly upon target systems and/or infrastructure; this may or may not include moves to obfuscate attribution of the attack to the attacker (i.e. through the use of proxies). Example: Operation Glowing Symphony - US intrusion into ISIS IT systems to disrupt their online propaganda efforts. Measures included collecting passwords, deleting files, throttling connection speeds and placing malware.[81] The result forced ISIS to abandon its network, setting back its online operations. Targeted malware to undermine target capability, either as a single domain measure or in conjunction with cross-domain measures. Example: Stuxnet attack on Iranian nuclear facilities (2008).[82]
	Prevention	Offensive cyber pre-positioning within the physical infrastructure to undermine target mobility. This includes intercepting internal messages, deleting passwords, and undermining the general integrity of target systems. Typically, this includes measures to conceal the attacker's identity, and make the attack resemble mundane IT issues. Example: Operation Synthetic Theology: USCYBERCOM preventive hacking/shutdown of Russian troll farm (IRA) infrastructure during the 2018 US midterm elections.[83] Incorporating built-in vulnerabilities into target infrastructure, that can be used in the event of potential conflict (vulnerabilities built into systems at the design stage, as opposed to inserted malware like Stuxnet). Example: Nitro Zeus US malware inside Iranian SCADA systems (2017).[84]
Coercion	Compellence	Use of ransomware by an attacker to compel a particular action from the victim, with the **threat of destructive action if demands are not met**; failure to comply may result in the destruction or publication of the hostage information. Although the current use of this is confined to non-

[81] USCYBERCOM After Action Assessments of Operation Glowing Symphony, NSA Archive, 22 November 2016: https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony
[82] An Unprecedented Look at Stuxnet, the World's First Digital Weapon, Kim Zetter, WIRED, 03 November 2014: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[83] Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections, Julian E. Barnes, New York Times, 26 February 2019: https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html
[84] US to Launch 'Nitro Zeus' Cyber Attack on Iran, Naveen Gou, Cybersecurity-Insider: https://www.cybersecurity-insiders.com/us-to-launch-nitro-zeus-cyber-attack-on-iran/

		state actors, it is theoretically possible the same could be employed at the state level. Example: North Korea's employment of the WannaCry ransomware in 2017, whose goal was ostensibly to extort payment from victims and retaliation against international sanctions. At the time, the difficulty of technical attribution allowed North Korea to operate with plausible deniability, avoiding the cost of escalating action.[85]
	Deterrence	*Communicating* offensive capability to the attacker, typically after a successful attack has already occurred. This can also include unilateral capacity building or collective defense with other cyber actors. The goal is to deter potential attackers through the threat of retaliation, the imposition of costs which outweigh the benefit of attack or increasing the risk for getting attributed and suffering possible counteractions. (Defensive) Example: US-Estonia Joint Cyber Platform following repeated Russian cyber-attacks upon Estonia. After a severe attack on Estonia's electrical grid in 2007, they have increasingly assumed a position as the symbol for NATO's collective cyber defense. The joint US-Estonian cyber threat intelligence platform seeks to bolster Estonian cybersecurity, and reiterate NATO's Article 5 as applying to cyberspace.[86] (Offensive) Example: Russian cyber-attack upon an Estonian power grid to communicate offensive capability (2007). Russian pre-positioning within US critical infrastructure (power grids, oil and gas pipelines, and water supplies).[87] Reciprocal US prepositioning within Russian critical infrastructure culminates in a cyber equivalent form of M.A.D (mutually assured 'disruption' in cyberspace).[88]
Protection	Defense	Reducing one's attack surface area – either through restricting certain networks or fully Balkanizing one's internet to prevent exposure to the target's influence (i.e. Chinese firewall and the Russian initiative to develop a national internet, called RuNet). Building active defensive measures by exposing the target's intentions, conveyed to both domestic and international observers. *Banning software and hardware (critical for the national vital infrastructure) from foreign companies.* This measure requires sensitive balancing between economic interests and principles (open market system) and security concerns. Example: Huawei 5G network banned by the US, Australia, and (mostly) the UK. Another example is the Kaspersky internet security and anti-virus

[85] Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea, White House Briefing, 19 December 2017,
[86] Estonia and the United States to Build a Joint Cyber Threat Intelligence Platform, E-Estonia, January 2020: https://e-estonia.com/estonia-united-cyber-threat-intelligence-platform/
[87] Russian Hackers Haven't Stopped Probing the US Power Grid, Lily Hay Newman, WIRED, 28 November 2018: https://www.wired.com/story/russian-hackers-us-power-grid-attacks/
[88] U.S. Escalates Online Attacks on Russia's Power Grid,David E. Sanger and Nicole Perlroth, New York Times, 15 June 2019: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

		software manufacturer. The EU Parliament has already singled out Kaspersky, just like the US, UK, Lithuania and the Netherlands.[89]
	Resilience	Making oneself robust against commonly known high volume exploits raise the cost of future attacks by preempting repeat use of exploits. This is typically accomplished via public-private partnerships to collate and mitigate known exploits (i.e. UK's Active Cyber Defense). Example: UK Active Cyber Defense (ACD): This public-private partnership, launched in 2016, involved the UK national cybersecurity center providing free protective technologies for private companies to improve their cyber defense and hygiene. Simultaneously, they collect metadata from companies which have been attacked, to better inform future cyber defense and build resilience.[90]
Persuasion	Inducement	Offering the sharing of intelligence about cyber capabilities.
	Assurance	Transparent outlining of one's offensive cyber capabilities and their operational mandate through published cyber strategies or other official channels. Communicating *how* one intends to operate in cyberspace and minimize uncertainty amongst potential adversaries. Example: The US, Australia, Netherlands, UK, and other European countries have published their offensive cyber capabilities, and outlined in national strategy documents their operational mandate, in order to communicate intentions and redlines to attackers.[91]
Cooperation	Entanglement	Communicating cross-domain countermeasures to potential cyber-attacks; linking cyber defense to other channels of interdependence that would be leveraged in response to an attack (i.e. economic sanctions in response to cyber-attack). This may not create sufficient costs to an attacker who is not already interdependent with the victim (i.e. North Korean cyber-attacks upon the international economic system). US including Chinese cyber theft accusations within its justification for imposing sanctions. Example: Shared physical infrastructure (i.e. fiber optic cables) inherently impart a degree of entanglement through interconnected interdependence.[92]
	Conciliation	Fostering exchanges of information – regular bilateral communication – in participation for subsequent deepening of relations.

[89] Protecting Europe against hybrid threats, Gustav Gressel, European Council on Foreign Relations pages, 25 June 2019
[90] Active Cyber Defence (ACD), National Cyber Security Centre, 2020: https://www.ncsc.gov.uk/section/products-services/active-cyber-defence
[91] Defining Offensive Cyber Capabilities, Tom Uren, Bart Hogeveen and Fergus Hanson, ASPI, 26 June 2018: https://www.aspi.org.au/report/defining-offensive-cyber-capabilities
[92] Strategic Anti-Access/Area Denial in Cyberspace, Alison Lawlor Russell, CCDCOE, 2015: https://ccdcoe.org/uploads/2018/10/Art-11-Strategic-Anti-Access-Area-Denial-in-Cyberspace.pdf

		Cooperation within international agreements to outline general rules for cyberspace (i.e. prohibiting attacks upon critical infrastructure). Sharing of cyber threat information within NATO.[93]
	Accommodation	Disclosure of cyber vulnerabilities (zero days), that could otherwise be weaponized against the target. This can also be communicated bilaterally to a target to assure them of peaceful intentions. Example: UK publishing of vulnerabilities equities process following calls from the Cybersecurity Tech Accord (2018).[94]

Table 6 Cyber measures

3.3 Military Domain

The Military domain enables the use of force for the purpose of policy. The domain can further be sub-divided along with geographic environments in which the force is applied: land, sea, air and space. The proliferation in the militarization of these environments ensures that military power can now be exercised at an unprecedented scale and speed. Military instruments remain the only ones via which violence and damage can be applied directly, without the requirement of some prior interconnectedness between the two parties.

Strategy	Type	Generic military measures
Control	Pre-emption	Surprise strike against the adversary's military capabilities. For example, Israeli pre-emptive air-strikes against the Egyptian air force on the ground (1967).[95] Alternatively, fait accompli – peacetime seizure of contested territory to get into an advantageous position. For example, the Russian seizure of Crimea in 2014.[96]
	Prevention	Surprise surgical strike against designated targets to undermine target capability *before* it becomes an imminent threat. For example Operation Opera/ Babylon: Israeli surgical airstrike on Iraqi nuclear reactor under construction (1981).[97] Similar preventative strikes against nascent Syrian nuclear facilities (2007), and planned operations against Iran (cancelled in lieu of the success of Stuxnet). In all instances, the targeted nuclear facilities were not operational (in development or near completion), making the strike *preventive* in nature, rather than preemptive.
Coercion	Compellence	A threat of military invasion through force positioning. American naval blockade and military buildup to compel Soviets during the Cuban missile

[93] A New Era for NATO Intelligence, NATO Review, 29 October 2019: https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html
[94] The UK Government Publishes a Vulnerability Equities Process in Line With Cybersecurity Tech Accord Call, Tech Accord, 21 December 2018: https://cybertechaccord.org/uk-gov-equities-process/.
[95] Jeremy Bowen, '1967 War: Six Days That Changed the Middle East', *BBC*, 5 June 2017, https://www.bbc.com/news/world-middle-east-39960461.
[96] Nikolai Petrov, 'Chronology of the Transformation of the Crimean Peninsula into a Russian Region', *Russian Politics and Law* 54, no. 1 (June 2016): 96–105, https://doi.org/10.1080/10611940.2015.1160720.
[97] Joshua Kirschenbaum, 'Operation Opera: An Ambiguous Success', *Journal of Strategic Security* 3, no. 4 (Winter 2010): 49–62, https://doi.org/10.5038/1944-0472.3.4.3.

		Crisis (1962).[98] Alternatively, a threat of military retaliation against civilian or military targets through force positioning. Russian Military exercises to deter Ukraine from conflict escalation (2014).
	Deterrence	Credibly established and communicated retaliatory capability (ideally overwhelming).[99] For example, North Korea threatened South Korea and the US with nuclear retaliation as a response to the joint military exercise of the latter.[100]
Protection	Defence	Hardening of military infrastructure – improving the defensive features of military systems so that they can thwart the adversary's attack. For example, the use of bunkers, trenches or concrete walls in contemporary wars in Afghanistan and Ukraine.[101]
	Resilience	Proliferation/ dispersions/ disaggregation of military infrastructure – insurance that even if some pieces get knocked out the system it can still function well (Defense in-depth logic). Ensuring redundant backup systems for critical infrastructure through such initiatives as the proliferation of military satellites in space to make them dispensable, and therefore a less desirable target.[102]
Persuasion	Inducement	Arms trade initiatives – inducing changes in behavior through the offers of military supplies, training, equipment and intelligence. This may be done to reinforce ties with a strategically important partner, induce a change in perception in a former enemy, or leverage a balance of power in the region. For example, the US trading arms to Saudi Arabia to support its stance against Iran; US support for Egypt during the Cold War.[103]
	Assurance	Conducting joint military exercises, typically with former adversaries, to communicate peaceful intent and transparency. For example, the NATO-Rostov Games.
Cooperation	Entanglement	Sharing risk for the use of military capabilities - the use would mutually harm both attacker and defender in the event of they're becoming involved in a general conflict. For example, mutual reliance upon key infrastructure within space (US-Russia/China).[104]

[98] Benjamin Schwarz, 'The Real Cuban Missile Crisis', January 2013, https://www.theatlantic.com/magazine/archive/2013/01/the-real-cuban-missile-crisis/309190/.
[99] Roger McDermott, 'The Kremlin's Strategy on Ukraine and Conflict De-Escalation', *Eurasia Daily Monitor* 11, no. 79 (April 2014), https://jamestown.org/program/the-kremlins-strategy-on-ukraine-and-conflict-de-escalation/.
[100] BBC, 'North Korea Threatens US and S Korea with Nuclear Strikes', *BBC*, 7 March 2016, https://www.bbc.com/news/world-asia-35741936.
[101] David Betz, 'World of Wallcraft: The Contemporary Resurgence of Fortification Strategies', *Infinity Journal* 6, no. 1 (Winter 2018): 18–22.
[102] Andrea Console, 'Space Resilience – Why and How?' (Joint Air Power Competence Centre, 2018), https://www.japcc.org/space-resilience-why-and-how/.
[103] Dominic Dudley, 'U.S. Arms Sales To The Middle East Have Soared In Value This Year', *Forbes*, 16 December 2019, https://www.forbes.com/sites/dominicdudley/2019/12/16/arms-sales-middle-east-soar/#687cefbffea8.
[104] Katarina Damjanov, 'Of Defunct Satellites and Other Space Debris: Media Waste in the Orbital Commons', *Science, Technology and Human Values* 42, no. 1 (2017): 166–85, https://doi.org/10.1177/0162243916671005.

	Conciliation	Arms control initiatives – getting rid of the specific weapon systems which may be seen as threatening. For example through Intermediate-Range Nuclear Forces Treaty (1988).[105]
	Accommodation	Withdrawal of troops away from the target's perceived sphere of influence. Alternatively, to surrender certain capabilities viewed as provocative by potential adversaries. For example, Budapest Memorandum - Ukraine's agreement to surrender its nuclear stockpile after the collapse of the USSR, in return for security assurances by Russia/US/UK.[106]

Table 7 Military measures

3.4 Economic Domain

The economic domain enables the use of finances or energy for the purposes of policy. Since both commodities are crucial for the everyday exercise of statecraft, the economic domain is a key enabler for the effective conduct of strategies in every other domain. In terms of adversarial use, the power of economic instruments depends on the relative interconnectedness of the respective entities. However, due to the ever-increasing interconnectedness of the public and private sector, the economic domain continues to grow in importance.

Strategy	Type	Generic economic measures
Control	Pre-emption	Blocking/ hindering resource distribution to hinder the adversary's access to immediate resources necessary to launch attacks. For example, Russian termination of gas supply for Ukraine (2015).[107]
	Prevention	Using economic/ financial sanctions with regards to import of critical weapon technology, in order to prevent the development of specific capabilities. For example, the US used economic sanctions against Iran to prevent the development of nuclear weapons (2018).[108]
Coercion	Force	**Threatening** the use of sanctions/ supply manipulation/ price increase in order to **change** the target's current behavior. For example, the US threatened to impose sanctions on Turkey if the latter continues with military actions in Syria (2019).[109]
	Deterrence	Threatening the use of sanctions/ supply manipulation/ price increase in order to **maintain** the target's current behavior. China has threatened

[105] NATO, 'NATO and the INF Treaty', *NATO* (blog), 2 August 2019, https://www.nato.int/cps/en/natohq/topics_166100.htm..
[106] Steven Pifer, 'Why Care about Ukraine and the Budapest Memorandum', *Brookings* (blog), 5 December 2019, https://www.brookings.edu/blog/order-from-chaos/2019/12/05/why-care-about-ukraine-and-the-budapest-memorandum/.
[107] BBC, 'Ukraine Closes Airspace to All Russian Planes', *BBC*, 25 November 2015, https://www.bbc.com/news/world-europe-34920207.
[108] ABC, 'Donald Trump Restores Iran Sanctions, Hitting Oil Exports over Its Support for Militant Groups', *ABC*, 2 November 2018, https://www.abc.net.au/news/2018-11-03/trump-and-iran-sanctions/10462528.
[109] Vivian Salama, Nancy A. Youssef, and Ian Talley, 'U.S. Threatens Turkey With Sanctions', *The Wall Street Journal*, 11 October 2019, https://www.wsj.com/articles/trump-readies-new-turkey-sanctions-11570817690.

		retaliation, implied as economic in nature, to dissuade the US from issuing new tariffs on Chinese goods.[110]
Protection	Defense	Hardening the energy infrastructure and calibrating supply chains to mitigate potential disruption from an adversary. Alternatively, ensuring the supply of critical goods remains politically neutral and does not become weaponized by a third-party adversary (i.e. US supply of semiconductors from Taiwan remain outside the remit of China's influence).
	Resilience	Developing alternative economic ties to decrease dependency upon a single vulnerable source plus stockpiling reserves of supplies in anticipation of future disruption. For example, Ukraine decreased its dependence on Russia by also importing gas from its neighbors such as Slovakia, Poland and Hungary (2019); the reliance on the US natural gas supply as a potential alternative to Russian-Europe energy monopoly.[111]
Persuasion	Inducement	Offering the forgiveness of debt in return for policy adjustment. For example, the EU may offer to forgive Greek debts or to postpone its payment in order to motivate more responsible domestic policies in Greece. Alternatively, it can offer a promise of entry into international markets, particularly energy markets, in return for certain policy changes. Example: US/EU JCPOA vis a vis Iran – nuclear disarmament in return for access to markets and oil markets, primarily to Europe.
	Assurance	Promising or delivering financial donations to alleviate the target's situation. For example, China sending food supplies to North Korea in order to demonstrate that it is a good ally.[112]
Cooperation	Entanglement	Deepening of economic interdependence. For example, a continuation of the ongoing entanglement of economic/ energy sectors between the US and China.[113]
	Conciliation	Removal of import tariffs/ domestic subsidies to increase foreign competition in respective markets. For example, EU elimination of tariffs under free trade agreements with Vietnam, Japan, Ukraine (on certain industrial goods).
	Accommodation	Accepting economic competition from adversaries, or their presence within one's own economy. For example, the acceptance of Huawei at European markets (in contrast to the US).[114]

Table 8 Economic measures

[110] Bob Davis and Josh Zumbrun, 'U.S. Slaps Higher Tariffs on Chinese Imports as Trade Talks Resume', 10 May 2019, https://www.wsj.com/articles/u-s-to-move-forward-with-china-tariffs-trump-says-11557424081.
[111] Kosatka, 'Ukraine Significantly Increased Gas Purchases in Europe in 2019', 10 January 2020, https://kosatka.media/en/category/gaz/analytics/ukraina-znachitelno-uvelichila-zakupki-gaza-v-evrope-v-2019-godu.
[112] Reality Check Team, 'North Korea: Who Is Sending Aid?', *BBC*, 20 June 2019, https://www.bbc.com/news/world-asia-48637518.
[113] Howard Wachter, 'US - China Financial Entanglements' (Amsterdam: TNI, 1 June 2005), https://www.tni.org/en/article/us-china-financial-entanglements.
[114] Foo Y. Chee, 'EU Deals Another Blow to U.S., Allowing Members to Decide on Huawei's 5G Role', *Reuters*, 29 January 2020, https://www.reuters.com/article/us-telecoms-5g-eu/eu-deals-another-blow-to-u-s-allowing-members-to-decide-on-huaweis-5g-role-idUSKBN1ZS163.

3.5 Legal Domain

The legal domain enables the use of law for the purposes of policy. The legal domain can be further subdivided into the realms of national and international law, both of which can be used and misused for political purposes. In comparison to other domains, the power of law is most dependent upon the perception and sincere commitment of the respective actor, and least dependent upon actual realities on the ground. Nonetheless, law can be a powerful instrument because it may convey a moral high-ground which then can be further capitalized on.

Strategy	Type	Generic legal measures
Control	Pre-emption	Withdrawal from a treaty in order to regain national control and being able to act autonomously (without consultation or restrictions) or to avoid interference and inspections by international bodies. For example, the US withdrawal from the Open Skies treaty.
	Prevention	Banning the developments of specific weapons. For example, the Biological Weapons Convention (BWC) which entered into force in 1975.[115]
Coercion	Compellence	Threats of legal sanctions to compel adversaries to start or return to abiding by the rules. For example, the ICC probe into Myanmar's crimes against the Rohingya; Palestinian Authorities threaten to file against Israel in the ICC if they refuse to negotiate land disputes in the West Bank.
	Deterrence	Threats of legal sanctions to dissuade the adversary from breaking the rule Legal precedents established in landmark international law cases (i.e. ICC/ICJ), may also inflict a deterrent effect upon other potential adversaries. Alternatively, this includes threats of prosecution within one's domestic legal jurisdiction if a target does not accept one's demands. For example, US threat of prosecuting ICC judges, and assistant organizations, in US courts in retaliation for their investigation into US war crimes in Afghanistan.[116]
Protection	Defense	Strengthening legal regulatory frameworks – outlining enforceable punitive measures for actors who deviate from legal frameworks. Refining frameworks to prevent misuse by members acting in bad faith. For example, reforming Interpol to prevent Russian lawfare - fraudulent arrest warrants against dissidents, non-abidance with organizational rules etc.
	Resilience	Supplementing legal rulings with committed norms, in order to reinforce a legal defense issue with different perspectives. Norms may also be employed as a precursor to international law for emerging issues (i.e. cyber) which lack a robust governing legal framework. For example, Paris Call for cyber norms/GCSC norms adopted by EU states etc.
Persuasion	Inducement	Promises allowing the target to participate in the development of new laws; encouraging multistakeholder input in the building of international law. For example, the UN Open Ended Working Group (UN OEWG).

[115] UNODA, 'Biological Weapons' (UN), accessed 13 May 2020, https://www.un.org/disarmament/wmd/bio/.
[116] BBC, 'John Bolton Threatens ICC with US Sanctions'.

	Assurance	Offering leniency to violators of the law to encourage/reassure that they may return to abidance without suffering punitive action. For example, offering former insurgents legal immunity in return for demobilization (i.e. Columbian FARC rebel negotiations).
Cooperation	Entanglement	Participation in legally binding multilateral treaties.
	Conciliation	Allowance for multiple interpretations of the same law; compromising specificity in order to achieve wider acceptance.
	Accommodation	Accepting some deviations from legal norms – that exceptions to the law may be tolerated. This conveys acceptance of a degree of legal ambiguity on certain issues. For example, Poland and Hungary as members of the EU not *wholly* committed to its democratic principles but they are still part of the union. This is similar to the position of Saudi Arabia in the UN Human Rights Council.

Table 9 Legal measures

4 From Single Domain To Cross-Domain Strategies: Issues to Consider

In this chapter we turn our attention to cross-domain strategies for countering hybrid threats. The cross-domain character of contemporary conflict strategies adds another layer of complexity to the portfolio of strategic options, namely the multiplicity of instruments through which the strategic efforts can be conducted. To help navigate this complexity, this chapter delineates five kinds of assessment that need to be conducted before, during and after the employment of strategies in the cross-domain context. These are: 1) costs and benefit assessment, 2) cross-domain orchestration, 3) proportionality, 4) signaling effects, and 5) legal and normative frameworks. These assessments shed light on, respectively, the effectiveness, the feasibility, the appropriateness, the perceptual, and the legitimacy of possible strategic options. They thus provide guidance on how to think about the salient issues in the selection and execution of cross-domain strategies in hybrid conflicts.

4.1 Cost-Benefit Assessment

The first assessment, the one that must be made at the very start of any strategic decision-making process, is the evaluation of the costs and benefits associated with the particular cross-domain strategy.[117] This assessment presupposes prior selection and prioritization of objectives. It is only once the political objectives are established that any action can be evaluated as beneficial or detrimental to its achievement. Every strategy, and each domain, has advantages and disadvantages that need to be carefully weighed against each other. It is relevant to start with the assessment of benefits because these should be directly related to the objectives that are pursued. The bottom line is that no matter how great the benefits are, if they do not contribute to the relevant objectives, then the strategy and the associated costs may be either irrelevant or outright damaging. The calculation of benefits in the cross-domain context needs to consider the potential interaction between instruments, which may enhance or degrade each other's effects. For example, the potential benefits of controlling strategies are likely to be enhanced when conducted across military, diplomatic and economic domains, because in all these forms the strategies drain away from the adversary's resources. On the other hand, coercive strategies conducted across domains may not enhance each other's potential because the adversary is likely to pay attention to the most dangerous threats and to ignore or neglect the rest of them. A similar logic applies to the assessment of costs in the cross-domain context. Controlling strategies exercised across military and economic domains are always bound to be expensive while those relying on the use of diplomacy and information may be cheaper in relative terms. The cost-benefit assessment should also consider the potential costs associated with risks attached to a particular course of action and its failure. In sum, the cost-benefit assessment takes into account the costs of potential risks and sheds light on the expected effectiveness of the strategy in the cross-domain context.

[117] The sequence of the kinds of assessment is debatable. One may argue that the more principal discussions of proportionality and legality should precede the more practical assessments of cost-benefit and feasibility of cross-domain orchestration. On the other hand, why enter into lofty legal and moral discussions about measures that cannot be practically implemented or have little added value? In any real-world application, however, the various assessment processes probably run in parallel and intertwined.

4.2 Cross-Domain Orchestration Assessment

This assessment concerns the practical orchestration of the strategy across domains. Strategy needs to be implemented in practice. Here the key questions relate to the identification and availability of sufficient means, of appropriate ways, and of practical coordination mechanisms for linking and tuning of actions across domains to create synergetic effects. No strategy can be exercised without means and the cross-domain context allows for a broad spectrum of options to choose from. For small and middle powers, the international context and the position of allies and friendly nations will need to be considered since actions are typically conducted within the context of international coalitions. First and foremost, it is crucial to know the priorities of others because these determine the character and the extent of effort the latter are willing to invest on their behalf. Relatedly, it is essential to know what sorts of means across domains do our allies have and which of these are they willing to employ in support of a chosen strategy. This all ties to the question of synchronization between ours and allied strategic practice. Cross-domain orchestration at both the international and the national level brings with it an assortment of additional challenges. Since cross-domain orchestration may include any or all of the diplomatic, information, cyber, economic, military and legal instruments, it is necessary to know who is responsible for the mobilization, coordination and employment of the particular domain specific instruments as well as which actors possess the mandate to employ these resources to pursue objectives in unlike domains. The complexity of orchestrating cross-domain instruments tends to be further exacerbated by the fact that responsibilities and capabilities are spread out over different government departments. It is therefore necessary to identify the mandate and the responsibilities for the use of resources in addition to the coordination mechanisms for how these means can be used, including how long and against what kind of threats.

4.3 Proportionality Assessment

This assessment is concerned with the appraisal of the cross-domain strategy's proportionality in relation to the particular challenge at hand. In order to do that, it is necessary to first and foremost identify the character of the challenge that is to be countered. Proportionality is then a subjective metric but it is generally a function of two distinct sources – instruments and effects. Proportionality of instruments relates to the character of the domains in and through which the strategy is employed. A basic level of proportionality can be achieved by using military instruments to counter military threats and non-military instruments to counter non-military threats. It also follows that, in general, using the military instrument to counter non-military threats is likely to be disproportional. The proportionality of effects is more complicated because the latter cannot be easily categorized and, therefore, contrasted. Nonetheless, it is possible to divide effects into physical and psychological ones respectively, a distinction that already gets us on the right way towards assessing their (dis)proportionality. Physical effects are more proportional to other physical effects while psychological effects are more proportional to psychological effects. At the same time, it is necessary to acknowledge that in the cross-domain context most instruments, most of the time, produce both physical and psychological effects. It is, therefore, necessary not only to assess the character of the effects but also their severity. For example, while military and economic control both produce physical effects, the

former tends to be more severe than the latter, in particular in the short run. Thus, it is possible to conduct preliminary assessments of proportionality of strategies and threats in the cross-domain context and it is necessary to do so in order to appraise the appropriateness of the strategy to the situation at hand. These points tie back to the escalation ladder introduced earlier – proportionality, though always subjectively perceived by the belligerents and never something objectively established – which is essential to navigate potential escalation dynamics during the conflict, whether that navigation is conducted unilaterally or mutually.

4.4 Signaling Assessment

This assessment pertains to the anticipation of how the adversary is likely to perceive the actions and what psychological effects will be produced by strategic signaling. The execution of every strategy signals a message, no matter whether that message is intended or not. For this reason, it is essential to appraise what any particular strategy signals to the adversary as well as to domestic and international audiences (including allies and other potential adversaries). The psychological effects of signaling largely depend on the cognitive processes of the respective audience and on the escalation potential of particular domains. For this reason, it is necessary to have some level of understanding of the particular belief systems and perceptions of the relevant audiences. At the same time, it is also crucial to understand that strategies conducted in and through some domains may appear less escalatory than those conducted in other domains. Signaling will be more complicated in some domains as opposed to others. It is comparatively easier to signal through military domains than through the cyber one because actions in the former change situation on the ground while the latter does not do so in an easily observable way. The solution to the signaling puzzle resides in the right combination of instruments so that these enhance each other's signaling potential. For example, coercion exercised through cyber instruments could be complemented by economic or military instruments so that the adversary is less likely to misunderstand or ignore the message. In sum, the assessment of effects produced by strategic signaling rooted in a good understanding of an opponents' belief system sheds light on the potential conversion rate between the use of strategies and the psychological consequences they are likely to create.

4.5 Legal and Normative Frameworks Assessment

The final assessment concerns the evaluation of the strategy concerning the relevant legal and normative frameworks, domestically and internationally. Here the first question is both whether the domestic legal framework allows for the selection of the strategy but also whether it allows for the prolonged exercise of the strategy. It is, therefore, necessary to assess which options are legal in particular domains but also across them. This assessment also relies on targeting – it is necessary to know what can and what cannot be targeted by all the instruments of statecraft involved in carrying out the strategy. For example, some legal frameworks may only allow for offensive cyberattacks to target military rather than civilian infrastructure. The second question is concerned with the legitimacy of the strategy from the perspective of both international law and international norms. It is first and foremost essential to appraise whether there is any existing international framework that regulate the conduct of the strategy. For example, in relation to the conduct of military operations, frameworks

such as The Law of Armed Conflict regulate the particulars to such an extent that they effectively limit the usefulness of such tools. Additionally, it is also important to assess whether the conduct of particular strategy conveys the emergence or propagation of a new norm of behavior or whether it falls within the framework of the existing norms. For example, the US has recently been promoting the norm of using diplomatic and economic coercion as a response to foreign, in this case Chinese, intellectual theft. In sum, the assessment of the strategy about normative frameworks reveals the permissibility and legitimacy of the strategic options.

4.6 Insights for the HCDS Game

The five assessments and the types of questions that need to be asked are summarized in the table below.

Five kinds of assessment in the formulation, selection and execution of cross domain strategies	
Core assessment question	**Particulars**
1. How does the cross-domain strategy fare in the cost/ benefit assessment?	• What are the political objectives? • What are the potential benefits and costs associated with the strategy? • What are the potential sources of failure across domains?
2. How can the strategy be executed and orchestrated in the cross- domain context?	• What sort/ form of support can we expect from our allies? • What means are available across all domains? • Who has the mandate and the responsibility to mobilize and use these respective means? • What are the specific limitations and opportunities associated with the employment of the particular means? • How can these means be synergistically employed across domains?
3. How proportional is the cross-domain strategy in relation to the threat?	• What is the character of the challenge? • Is the character of the instruments employed proportional to the character of the challenge? • Is the character of the potential effects proportional to the severity of the challenge?
4. What are the likely signaling effects of the strategy?	• What are the audience's belief system and perceptions? • How escalatory is the strategy in different domains to be perceived by the adversary?

5. What is the relationship of the particular cross-domain strategy to the relevant domestic and international legal and normative frameworks?	• What is the domestic and international legal framework covering the actions included in the strategy? • What international norms pertain to the exercise of the strategy? • How does the strategy shape international norms?

Table 10 Five kinds of assessment in the formulation, selection and execution of cross-domain strategies

4.7 Conclusion

The goal of this project is to offer a menu of strategies that can be used to actively counter hybrid threats. Accordingly, we have developed a set of five strategies that can be employed simultaneously or sequentially to counter hybrid threats. These strategies are cooperation, persuasion, protection, coercion and control, which can be exercised through and across six different domains: diplomatic, information, cyber, economic, military and legal. The detailed overview of strategies provided in chapter 3 offers foundations for clear thinking but also for practical strategic posture construction, both of which are integral components in countering hybrid threats.

Three points warrant special attention. First, strategies vary in their escalation potential. Cooperation is the least escalatory strategy because it aims to create win-win situations. Persuasion is more escalatory because it is about submitting the adversary to one's own will but at the same time it grants the latter some benefits to enjoy. Protection is on the next escalation level because the adversary gains nothing from its conduct, though it also does not lose anything. Coercion is yet more escalatory because it seeks to produce clear win – lose situations. Finally, controlling strategies are the most escalatory ones because they seek to impose defeat on the adversary. The escalation dynamics associated with the individual strategies should always be taken into account because their appreciation allows for escalation management.

Second, the effectiveness of the strategies varies with the character of the domain through which they are conducted. For example, while diplomacy is as old as statecraft itself, modern communication technologies allow for negotiations to take place faster as well as more frequently. Likewise, the contemporary information environment presents aggravated asymmetries between offense and defense, as the attack surface of open societies is relatively large and vulnerable to aggressive state and criminal non-state actors. Similarly, the growing prominence of cyberspace as a domain presents new issues to traditional deterrence, given its novel asymmetries of ambiguity and relatively inexpensive offense, and expensive and rarely effective defense. Meanwhile, the military instrument remains a class of its own because it is the only one via which violence and damage can be applied directly. In contrast, the economic domain continues to grow in importance due to the ever-increasing interconnectedness of the public and private sector. In comparison to other domains, the shaping power of law is most dependent upon the perception and commitment of all parties. But even in an antagonized world, law can be a relevant instrument, if only because abiding by its tenets may convey a moral high-ground which can be capitalized on. Each domain, therefore, offers

opportunities and limitations that need to be considered before any specific strategy is selected.

Third and finally, any cross-domain employment of strategies is complicated and therefore requires a holistic assessment. Strategies should be evaluated in terms of the benefits they may produce and in the costs they may incur. However, it is imperative to start with the benefits, because if these do not contribute to the overall objectives, then the strategy itself is irrelevant. The latter also holds when the synergetic orchestration of a cross-domain strategy cannot realistically be implemented. Additionally, proportionality of strategies to the character and the severity of the challenge need to be evaluated, both in terms of the instruments employed and the effects produced. Moreover, the psychological effects of strategic signaling need to be anticipated by zooming in on the adversary's and international community's perceptions and beliefs but also by appreciating the different escalatory logics of distinct domains. And finally, the domestic and international normative and legal frameworks that may allow or hinder strategic exercise need to be considered. An assessment of all of these aspects, individually and in combination, does not guarantee strategic success, but provides the most reliable way against strategic failure.

The theoretical propositions above need to be further tested in an interactive practice. While in theory the logic behind the framework may seem crystal clear, strategic practice may falsify some of its assumptions or it may motivate further adjustments or refinements of its constituting elements. For this purpose, we will use a simulation environment in the form of a table-top game to shed light on how the strategies work in a simulated competitive setting. The findings gained from this exercise will help refine the framework and inform the crafting of effective cross-domain strategies in the real world.

Bibliography

NATO. 'A Short History of NATO'. Accessed 13 May 2020. https://www.nato.int/cps/en/natohq/declassified_139339.htm.

ABC. 'Donald Trump Restores Iran Sanctions, Hitting Oil Exports over Its Support for Militant Groups'. *ABC*, 2 November 2018. https://www.abc.net.au/news/2018-11-03/trump-and-iran-sanctions/10462528.

Adamsky, Dmitry. 'Cross-Domain Coercion: The Current Russian Art of Strategy'. Security Studies Center, 2015. http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf.

Almog, Doron. 'Cumulative Deterrence and the War on Terrorism'. *Parameters* 34, no. 4 (Winter 2004): 4–19.

Art, Robert J., and Kelly M. Greenhill. 'Coercion: An Analytical Overview'. In *Coercion: The Power to Hurt in International Politics*, edited by Kelly M. Greenhill and Peter Krause, 1 edition., 3–32. New York, NY: Oxford University Press, 2018.

Baylis, John. 'The Concept of "Tailored Deterrence" in the "Second Nuclear Age"'. *St Antony's International Review* 4, no. 2 (February 2009): 8–23.

BBC. 'John Bolton Threatens ICC with US Sanctions'. *BBC*, 11 September 2018. https://www.bbc.com/news/world-us-canada-45474864.

———. 'North Korea Threatens US and S Korea with Nuclear Strikes'. *BBC*, 7 March 2016. https://www.bbc.com/news/world-asia-35741936.

———. 'Ukraine Closes Airspace to All Russian Planes'. *BBC*, 25 November 2015. https://www.bbc.com/news/world-europe-34920207.

Betz, David. 'World of Wallcraft: The Contemporary Resurgence of Fortification Strategies'. *Infinity Journal* 6, no. 1 (Winter 2018): 18–22.

Biddle, Tami D. 'Coercion Theory: A Basic Introduction for Practitioners'. *Texas National Security Review* 3, no. 2 (Spring 2020). https://tnsr.org/2020/02/coercion-theory-a-basic-introduction-for-practitioners/.

Borghard, Erica D., and Jacquelyn Schneider. 'Israel Responded to a Hamas Cyberattack with an Airstrike. That's Not Such a Big Deal.' *Washington Post*, 9 May 2019. https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/.

Bowen, Jeremy. '1967 War: Six Days That Changed the Middle East'. *BBC*, 5 June 2017. https://www.bbc.com/news/world-middle-east-39960461.

Brantly, Aaron. 'Back to Reality: Cross Domain Deterrence and Cyberspace'. Boston: Virginia Tech, 2018. https://vtechworks.lib.vt.edu/bitstream/handle/10919/85386/Brantly-Back2Reality-APSA-DRAFT.pdf?sequence=1&isAllowed=y.

Brinkel, Theo. 'The Resilient Mind-Set and Deterrence'. In *Netherlands Annual Review of Military Studies*, edited by Frans Osinga and Paul Ducheine, 19–38. The Hague: Asser Press, 2017.

Chee, Foo Y. 'EU Deals Another Blow to U.S., Allowing Members to Decide on Huawei's 5G Role'. *Reuters*, 29 January 2020. https://www.reuters.com/article/us-telecoms-5g-eu/eu-deals-another-blow-to-u-s-allowing-members-to-decide-on-huaweis-5g-role-idUSKBN1ZS163.

Console, Andrea. 'Space Resilience – Why and How?' Joint Air Power Competence Centre, 2018. https://www.japcc.org/space-resilience-why-and-how/.

Cullen, Patrick, and Njord Wegge. 'Countering Hybrid Warfare'. Shrivenham: Development, Concepts and Doctrine Centre, March 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf.

Damjanov, Katarina. 'Of Defunct Satellites and Other Space Debris: Media Waste in the Orbital Commons'. *Science, Technology and Human Values* 42, no. 1 (2017): 166–85. https://doi.org/10.1177/0162243916671005.

D'Arcy, John, and Tejaswini Herath. 'A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings'. *European Journal of Information Systems* 20, no. 1 (June 2011): 643–58. https://doi.org/10.1057/ejis.2011.23.

Davis, Bob, and Josh Zumbrun. 'U.S. Slaps Higher Tariffs on Chinese Imports as Trade Talks Resume', 10 May 2019. https://www.wsj.com/articles/u-s-to-move-forward-with-china-tariffs-trump-says-11557424081.

Davis, Patricia A. *The Art of Economic Persuasion: Positive Incentives and German Economic Diplomacy Kindle Edition*. Ann Arbor: University of Michigan Press, 1999.

De Spiegeleire, Stephan, Khrystyna Holynska, Yar Batoh, and Tim Sweijs. 'Reimagining Deterrence: Towards Strategic (Dis)Suasion Design'. The Hague: The Hague Centre for Strategic Studies, March 2020.

Dudley, Dominic. 'U.S. Arms Sales To The Middle East Have Soared In Value This Year'. *Forbes*, 16 December 2019. https://www.forbes.com/sites/dominicdudley/2019/12/16/arms-sales-middle-east-soar/#687cefbffea8.

Efraim, Inbar, and Eitan Shamir. '"Mowing the Grass": Israel'sStrategy for Protracted Intractable Conflict'. *Journal of Strategic Studies* 37, no. 1 (February 2014): 65–90. https://doi.org/10.1080/01402390.2013.830972.

Flanagan, Stephen, J, Jan Osburg, Anika Binnendijk, Marta Kepe, and Andrew Radin. *Deterring Russian Aggression in the Baltic States Through Resilience and Resistance*. Santa Monica: RAND Corporation, 2019.

Freedman, Lawrence. *Deterrence*. Cambridge: Polity Press, 2004.

Fridman, Ofer. *Russian 'Hybrid Warfare': Resurgence and Politicization*. Oxford: Oxford University Press, 2018.

Gardner, Hall. 'Hybrid Warfare: Iranian and Russian Versions of "Little Green Men" and Contemporary Conflict'. Rome: NATO Defense College, December 2015. https://css.ethz.ch/en/services/digital-library/publications/publication.html/195396.

George, Alexander, and Graham Stuart. *Forceful Persuasion: Coercive Diplomacy as an Alternative to War*. Washington: United States Institute of Peace, 1992.

Glaser, Charles L. *Rational Theory of International Politics*. Princeton: Princeton University Press, 2010.

Gray, Colin S. 'Deterrence and Regional Conflict: Hopes, Fallacies, and "Fixes"'. *Comparative Strategy* 17, no. 1 (1998): 45–62. https://doi.org/10.1080/01495939808403131.

Hartmann, Uwe. 'The Evolution of the Hybrid Threat, and Resilience as a Countermeasure'. Zurich: Center for Security Studies, October 2017. https://css.ethz.ch/en/services/digital-library/articles/article.html/3eadb4fb-09de-4b79-93b1-af1ee4117a0d/pdf.

Hoffman, Frank G. 'Conflict in the 21st Century: The Rise of Hybrid Wars'. Arlington: Potomac Institute for Policy Studies, December 2007.

———. 'Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges'. *PRISM* 7, no. 4 (November 2018): 30–47. https://doi.org/N/A.

Hybrid CoE. *Deterring Hybrid Threats: A Playbook for Practitioners.* Helsinki: The European Centre of Excellence for Countering Hybrid Threats, 2020.

'In Defense of Deterrence | RealClearDefense'. Accessed 2 June 2020. https://www.realcleardefense.com/articles/2020/04/30/in_defense_of_deterrence_115237.html.

Johnson, Robert. 'Hybrid War and Its Countermeasures: A Critique of the Literature'. *Small Wars and Insurgencies* 29, no. 1 (December 2017): 141–63.

Kahn, Herman. *On Escalation: Metaphors and Scenarios*. Santa Barbara: Praeger, 1965.

Kello, Lukas. *The Virtual Weapon and International Order*. Yale: Yale University Press, 2017.

Kelman, Herbert C. 'Social-Psychological Dimensions of International Conflict'. In *Peacemaking in International Conflict: Methods and Techniques*, edited by William Zartman, 2nd ed., 61–110. Washington: United States Institute of Peace, 2007.

Kirschenbaum, Joshua. 'Operation Opera: An Ambiguous Success'. *Journal of Strategic Security* 3, no. 4 (Winter 2010): 49–62. https://doi.org/10.5038/1944-0472.3.4.3.

Kosatka. 'Ukraine Significantly Increased Gas Purchases in Europe in 2019', 10 January 2020. https://kosatka.media/en/category/gaz/analytics/ukraina-znachitelno-uvelichila-zakupki-gaza-v-evrope-v-2019-godu.

Krepinevich, Andrew F. 'The Eroding Balance of Terror: The Decline of Deterrence'. *Foreign Affairs*, February 2019. https://www.foreignaffairs.com/articles/2018-12-11/eroding-balance-terror.

Lindsay, Jon R, and Erik Gartzke. 'Introduction: Cross-Domain Deterrence, From Practice to Theory'. In *Cross-Domain Deterrence: Strategy in an Era of Complexity*, edited by Erik A. Gartzke and Jon R. Lindsay, 1–26. Oxford: Oxford University Press, 2019.

Long, William. *Economic Incentives and Bilateral Cooperation*. Ann Arbor: University of Michigan Press, 1996.

Mallory, King. 'New Challenges in Cross-Domain Deterrence'. Product Page. Santa Monica: RAND Corporation, 2018. https://www.rand.org/pubs/perspectives/PE259.html.

Mazarr, Michael, Arthur Chan, Alyssa Demus, Bryan Frederick, Alireza Nader, Stephanie Pezard, Julia Thompson, and Elina Treyger. *What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression*. RAND Corporation, 2018. https://doi.org/10.7249/RR2451.

Mazarr, Michael J. 'Understanding Deterrence'. Product Page, 2018. https://www.rand.org/pubs/perspectives/PE295.html.

McDermott, Roger. 'The Kremlin's Strategy on Ukraine and Conflict De-Escalation'. *Eurasia Daily Monitor* 11, no. 79 (April 2014). https://jamestown.org/program/the-kremlins-strategy-on-ukraine-and-conflict-de-escalation/.

McDonald-Gibson, Charlotte. 'Ukraine Crisis: EU Threatens Russia with New Economic Sanctions'. *The Independent*, 27 January 2015. https://www.independent.co.uk/news/world/europe/ukraine-crisis-eu-threatens-russia-with-new-economic-sanctions-10006736.html.

Mearsheimer, John. *Conventional Deterrence*. Ithaca: Cornell University Press, 1985.

Milevski, Lukas. 'Revisiting J.C. Wylie's Dichotomy of Strategy: The Effects of Sequential and Cumulative Patterns of Operations'. *Journal of Strategic Studies* 35, no. 2 (January 2012): 223–42. https://doi.org/10.1080/01402390.2011.563919.

Monaghan, Sean. 'Countering Hybrid Warfare'. *PRISM* 8, no. 2 (2019): 82–99.

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe. *Gaining Competitive Advantage in the Gray Zone*. Santa Monica: RAND Corporation, 2019.

Murray, Williamson, and Peter R. Mansoor, eds. *Hybrid Warfare*. Cambridge: Cambridge University Press, 2012.

NATO. 'Collective Defence - Article 5'. North Atlantic Treaty Organization, 2019. https://www.nato.int/cps/en/natohq/topics_110496.htm.

———. 'International Observers Visit Exercise Trident Juncture 2018'. *NATO* (blog), 1 November 2018. https://www.nato.int/cps/en/natohq/news_160033.htm.

———. 'NATO and the INF Treaty'. *NATO* (blog), 2 August 2019. https://www.nato.int/cps/en/natohq/topics_166100.htm.

Nye, Joseph S. 'Deterrence and Dissuasion in Cyberspace'. *International Security* 41, no. 3 (January 2017): 44–71. https://doi.org/10.1162/ISEC_a_00266.

Petrov, Nikolai. 'Chronology of the Transformation of the Crimean Peninsula into a Russian Region'. *Russian Politics and Law* 54, no. 1 (June 2016): 96–105. https://doi.org/10.1080/10611940.2015.1160720.

Pifer, Steven. 'Why Care about Ukraine and the Budapest Memorandum'. *Brookings* (blog), 5 December 2019. https://www.brookings.edu/blog/order-from-chaos/2019/12/05/why-care-about-ukraine-and-the-budapest-memorandum/.

Radin, Andrew. 'Hybrid Warfare in the Baltics'. Product Page. Santa Monica: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1577.html.

Reality Check Team. 'North Korea: Who Is Sending Aid?' *BBC*, 20 June 2019. https://www.bbc.com/news/world-asia-48637518.

Reuters. 'Turkey Shouldn't Coerce Greece, Europe over Migrants: Greek PM'. *Reuters*, 8 September 2019. https://www.reuters.com/article/us-greece-pm-policy-turkey/turkey-shouldnt-coerce-greece-europe-over-migrants-greek-pm-idUSKCN1VT0DB.

Rid, Thomas. 'Deterrence beyond the State: The Israeli Experience'. *Contemporary Security Policy* 33, no. 1 (April 2012): 124–47. https://doi.org/10.1080/13523260.2012.659593.

Rock, Stephen R. *Appeasement in International Politics*. Lexington: University Press of Kentucky, 2000.

Rozin, Paul, and Edward B. Royzman. 'Negativity Bias, Negativity Dominance, and Contagion'. *Personality and Social Psychology Review* 5, no. 4 (2001): 296–320.

Rühle, Michael. 'Deterring Hybrid Threats: The Need for a More Rational Debate'. NDC Policy Brief. Rome: NATO Defense College, 9 July 2019. http://www.ndc.nato.int/news/news.php?icode=1335.

———. 'NATO's Response to Hybrid Threats'. Washington: National Institute for Public Policy, 4 November 2019. https://www.nipp.org/2019/11/04/ruhle-michael-natos-response-to-hybrid-threats/.

Salama, Vivian, Nancy A. Youssef, and Ian Talley. 'U.S. Threatens Turkey With Sanctions'. *The Wall Street Journal*, 11 October 2019. https://www.wsj.com/articles/trump-readies-new-turkey-sanctions-11570817690.

Schelling, Thomas C. *Arms and Influence*. 2nd ed. New Haven: Yale University Press, 2008.

Schwarz, Benjamin. 'The Real Cuban Missile Crisis', January 2013. https://www.theatlantic.com/magazine/archive/2013/01/the-real-cuban-missile-crisis/309190/.

Singer, David J. 'Inter-Nation Influence: A Formal Model'. *The American Political Science Review* 57, no. 2 (June 1963): 420–30. https://doi.org/10.2307/1952832.

Snyder, Glenn H. *Deterrence and Defense: Toward a Theory of National Security.* First Edition. Princeton: Princeton University Press, 1961.

Stein, Janice Gross. 'Threat Perception in International Relations'. In *The Oxford Handbook of Political Psychology*, 2nd ed., 364–94. Oxford: Oxford University Press, 2013.

Stoker, Donald, and Craig Whiteside. 'Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking'. *Naval War College Review* 73, no. 1 (Winter 2020): 1–37. https://doi.org/N/A.

Sweijs, Tim, and Samuel Zilincik. 'Cross Domain Deterrence and Hybrid Conflict'. The Hague Centre for Strategic Studies, 2019. https://hcss.nl/sites/default/files/files/reports/Cross%20Domain%20Deterrence%20-%20Final.pdf.

Tor, Uri. '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence' 40, no. 1–2 (2015): 92–117.

UNODA. 'Biological Weapons'. UN. Accessed 13 May 2020. https://www.un.org/disarmament/wmd/bio/.

Vince, Robert J. 'Cross-Domain Deterrence Seminar Summary Notes'. Government & Nonprofit. Livermore: Center for Global Security Research, May 2015. https://www.slideshare.net/LivermoreLab/summary-notes-47797997.

Wachter, Howard. 'US - China Financial Entanglements'. Amsterdam: TNI, 1 June 2005. https://www.tni.org/en/article/us-china-financial-entanglements.

Williams, Greg. 'An Irish Entrepreneur and Bono Are Fixing the PPE Crisis'. *Wired*, 16 April 2020. https://www.wired.co.uk/article/ppe-shortage.