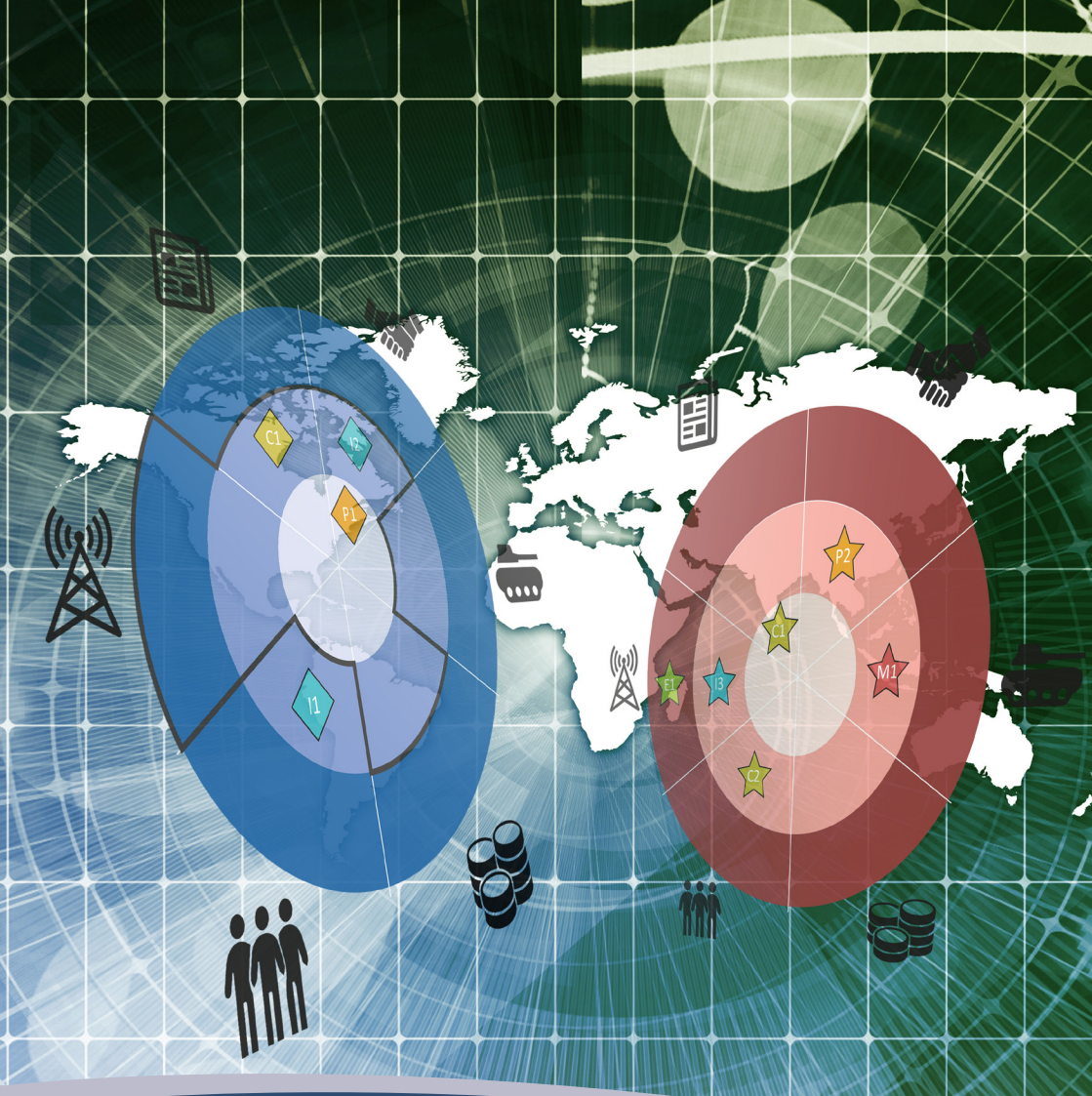


MCDC Countering Hybrid Warfare Project:

Countering Hybrid Warfare

March 2019

MCDC
Multinational Capability Development Campaign

MCDC Countering Hybrid Warfare Project:

Countering Hybrid Warfare

A Multinational Capability Development Campaign project

Distribution statement

Primary authors:

Editor, project lead: Sean Monaghan, Development, Concepts and Doctrine Centre, sean.monaghan105@mod.gov.uk

Project lead: Dr Patrick Cullen, Senior Research Fellow, NUPI, pc@nupi.no

Project lead: Dr Njord Wegge, Senior Research Fellow, NUPI, njordw@nupi.no

A full list of contributors to this project can be found at the end of the handbook on page 87.

Executive summary

Hybrid warfare is the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects. The challenge presented by revisionist actors who exploit hybrid warfare has a broad impact across societies, national government and multinational institutions.

The purpose of this handbook is to inform national and multinational security and defence policy by developing conceptual guidance for countering hybrid warfare. It builds upon previous guidance on understanding hybrid warfare. This handbook describes a framework for countering hybrid warfare based on the following components.

Set realistic strategic goals ranging from: maintaining the capacity for independent action; dissuading or deterring an adversary from hybrid aggression; through to disrupting or preventing an adversary from further hybrid aggression.

Identify appropriate thresholds for taking action. These may vary according to the type of aggression or the vulnerability being targeted and the capacity for counter action.

Design and implement a strategy based on the three components of detect, deter and respond.

- Detect. This component addresses the problem of detecting hybrid threats or attacks in the first place. It requires updating warning intelligence to monitor 'known unknowns' through indicators and warnings and discovering 'unknown unknowns' through pattern recognition and anticipation.

- Deter. This component addresses the deterrence of hybrid aggressors – or 'hybrid deterrence'. Deterring hybrid aggressors can be done, but it requires building on traditional deterrence to pursue credible measures through creative horizontal escalation, tailored and communicated to the aggressor, that are balanced between deterrence by denial – including resilience – and punishment.

- Respond. This component addresses how to respond to hybrid threats or attacks and offers a framework for doing so. The decision to respond by implementing appropriate actions and measures can be taken at any stage in the hybrid threat cycle, from identifying potential vulnerabilities that require resilience-building activity to punitive measures taken in response to a hybrid attack.

Develop the institutional machinery for implementing these measures through national governments and multinational institutions to make sure it is fit for purpose.

An overview of this framework is provided in Figure 1 on the opposite page. Tools to visualize the role each component plays in countering hybrid warfare are provided throughout the handbook.

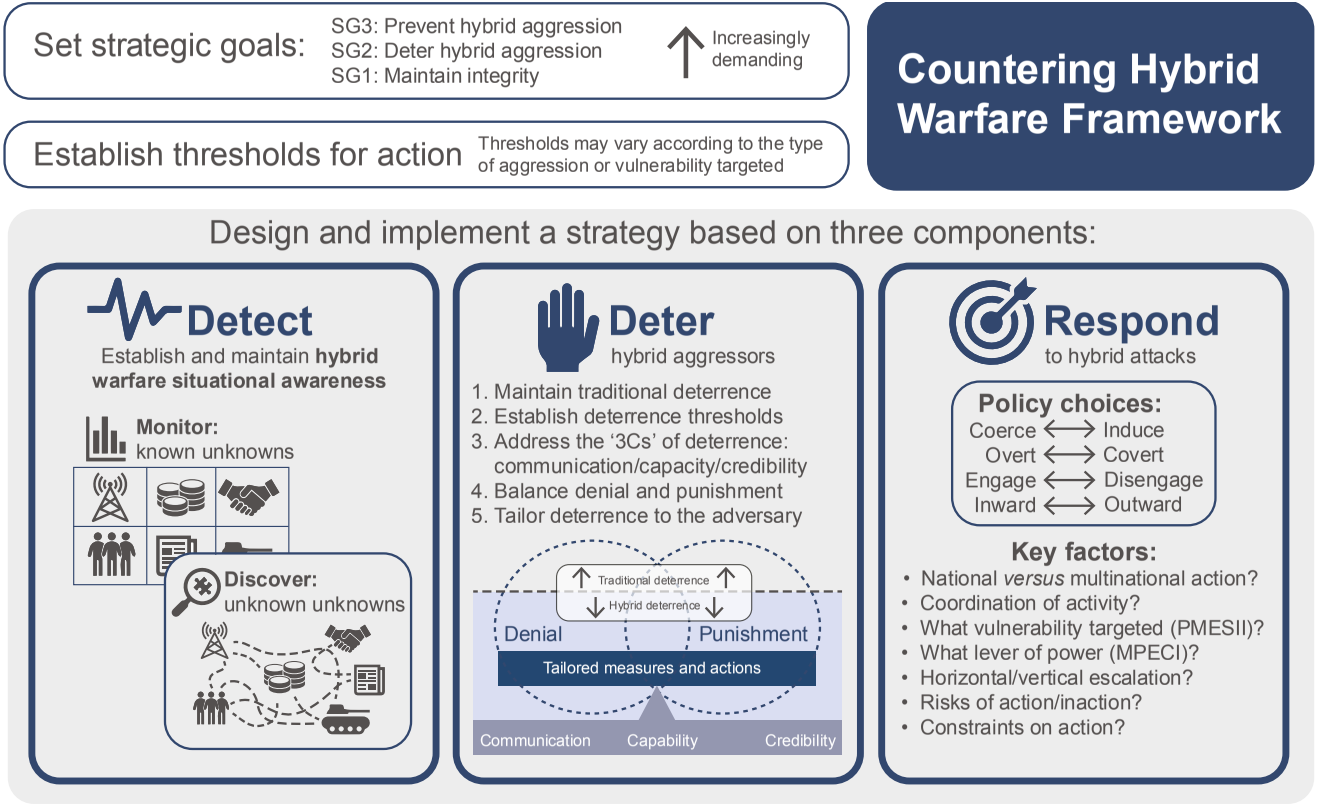


Figure 1 – The Countering Hybrid Warfare Framework

Contents

> Hybrid warfare describes the problem, not a solution.

MCDC, (2017), *Understanding Hybrid Warfare*

Introduction

What is the MCDC Countering Hybrid Warfare project?

The Multinational Capability Development Campaign (MCDC[1]) Countering Hybrid Warfare (CHW) project aims to help national and multinational security and defence decision-makers understand and counter hybrid warfare.

The first phase of the project (CHW1) established an understanding of hybrid warfare. This understanding was articulated in two key outputs: an information note – *What is Hybrid Warfare?,*[2] referred to as the 'Baseline Assessment', which addressed existing concepts of hybrid warfare and established a common language for describing it; and a handbook – *Understanding Hybrid Warfare,*[3] referred to as the 'Analytical Framework', which offered a conceptual and visual model to help understand hybrid warfare.

This handbook represents the findings of the second phase of the project (CHW2), which builds on the previous phase to develop conceptual and policy guidance for countering hybrid warfare.[4] Although its aim is to inform multinational policy, it does not represent national policy.

Purpose

CHW1 concluded that 'hybrid warfare describes the problem, not a solution'. The purpose of this handbook is therefore to inform multinational policy by developing conceptual guidance for countering hybrid warfare. It is organized into six chapters and four annexes.

- Chapters 1 and 2 recap the understanding of hybrid warfare from

1 The Multinational Capability Development Campaign (MCDC) enables multinational cooperation in addressing shared capability challenges. Further detail can be found at https://wss.apan.org/s/MCDCpub/default.aspx

2 MCDC Countering Hybrid Warfare Project, (2017), Information Note, *What is Hybrid Warfare?* A link to all information notes is available at Annex A.

3 MCDC Countering Hybrid Warfare Project, (2017), *Understanding Hybrid Warfare*, available at https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare

4 Phase 2 of the MCDC Countering Hybrid Warfare (CHW) project ran from June 2017 to December 2018. It had 14 member nations (Austria, Canada, Czech Republic, Denmark, Germany, Spain, Finland, United Kingdom, Netherlands, Norway, Poland, Republic of Korea, Switzerland and the United States) and involved the European Union, North Atlantic Treaty Organization and the Countering Hybrid Threats Centre of Excellence (Hybrid COE).

CHW1 and develops the outline CHW Framework.

- Chapters 3, 4 and 5 develop guidance for the three key components of the CHW Framework – detecting hybrid warfare, deterring hybrid aggressors and responding to hybrid attacks.

- Chapter 6 offers guidance for implementing these measures through national governments and multinational institutions.

- Annex A provides a list of information notes, research papers and case studies referred to throughout the handbook.

- Annex B visualizes three generic examples of countering hybrid warfare using the tools introduced in the handbook.

- Annex C provides a brief outline of the current state of countering hybrid warfare policy.

- Annex D summarises the key findings from a fictional scenario-based table-top exercise and matrix game.

Taken together, these chapters and annexes form a handbook to provide nations and institutions with the tools and guidance to develop the policy and strategy required to counter hybrid warfare. An overall CHW Framework, which brings all of the key ideas together onto one page, can be found on page 5.

Methodology

This handbook is based on original research and analysis from contributing MCDC member nations. Several research papers have been published as CHW 'Information Notes' to explain key concepts and innovations in more detail – these are referred to throughout the handbook. Several case studies were also produced to gain empirical insight and test the CHW Framework. The handbook uses a wide variety of empirical reference points and case studies – rather than focusing on one or two actors or examples – to reflect the widespread, enduring and evolving threat posed by hybrid warfare to international stability. The key ideas and concepts were discussed and refined during five project workshops. The final workshop included a fictional scenario-based table top exercise and matrix game to help test and refine the CHW Framework.

This handbook takes the same ‘generic’ approach to conceptual guidance as CHW1: it is meant to be applied by any nation or institution to their own situation. The handbook also relies throughout on visualisation and schematics to make a complex and challenging subject as simple and intuitive as possible.

> Hybrid warfare is the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects.

MCDC, (2017), *Understanding Hybrid Warfare*

Chapter 1

Understanding hybrid warfare

In CHW1 a conceptual model was developed for understanding hybrid warfare. The model was agnostic to the type of aggressor (for example, state or non-state actor) but focused on state-actors as the target.[5] It was based on the following key characteristics.

- The combined use of multiple instruments of power to achieve asymmetry through targeting an expanded range of vulnerabilities.
- A synchronized attack package that exploits both horizontal and vertical axes of escalation.[6]
- An emphasis on creativity and ambiguity to achieve synergistic effects (including in the cognitive domain).

The model describes how an actor engaging in hybrid warfare may use a wide range of military, political, economic, civilian and informational (MPECI) instruments of power aimed at the political, military, economic, social, informational and infrastructure (PMESII) vulnerabilities of a target system, to escalate in 'vertical' and 'horizontal' terms to achieve the desired goals while avoiding or complicating decisive counteraction. The instruments of power and vulnerabilities are shown in Figure 1.1, while the concept of synchronizing the instruments of power is visualized in Figure 1.2.

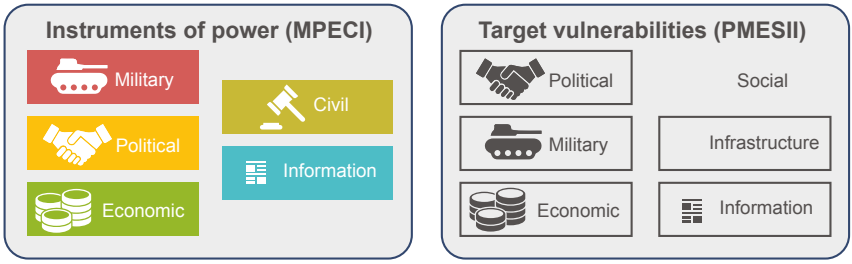


Figure 1.1 – MPECI instruments of power and PMESII target vulnerabilities

5 For more detail on why an actor-agnostic approach was taken, see MCDC, (2017), *Understanding Hybrid Warfare*, page 8; and MCDC, (2017), Information Note, *What is Hybrid Warfare?*, pages 2-3.

6 A 'synchronized attack package' is described as 'specific MPECI (military, political, economic, civil and informational) means that are synchronized and tailored to specific vulnerabilities that are used in a hybrid warfare attack', *Understanding Hybrid Warfare*, page 32.

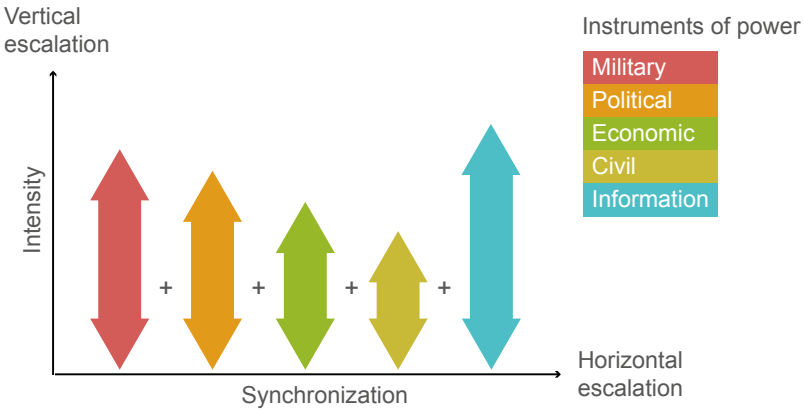


Figure 1.2 – The synchronized vertical and horizontal escalation characteristic to hybrid warfare

An analytical framework was also developed to demonstrate and visualize a hybrid attack. It focused on the PMESII vulnerabilities of the target, the ability of the aggressor to synchronize a wide variety of MPECI instruments of power, and the effects created by these actions. Visualized in Figure 1.3, it is based on the following three interdependent elements:

- critical functions and vulnerabilities;
- synchronization of means (horizontal escalation); and
- effects and non-linearity.

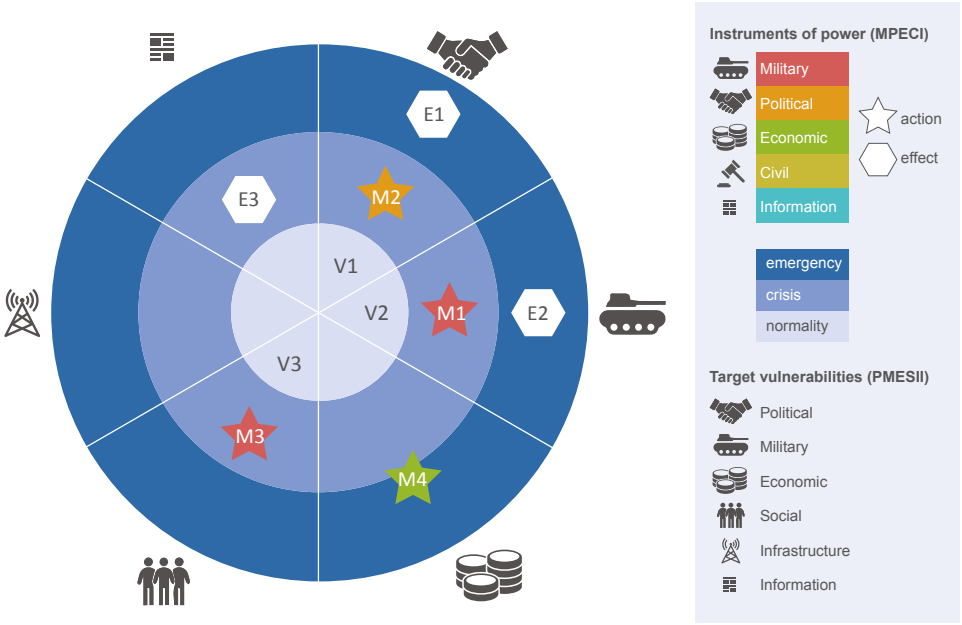


Figure 1.3 – Visualizing hybrid warfare

This framework incorporates all three elements to describe hybrid warfare as: the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects.[7]

7 MCDC, (2017), *Understanding Hybrid Warfare,* page 8.

> The potential for hybrid warfare to create destabilizing effects in the international system requires a strategic response.

Chapter 2

Countering hybrid warfare

> Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them.
>
> Jen Stoltenberg, NATO Secretary General, 2015

While the previous handbook focused on understanding hybrid warfare, this one is about countering it. Although the term hybrid warfare is used to explain the overall concept, a hybrid attack may not necessarily include the use of armed force.

The use of the term 'warfare' in this handbook is simply intended to signify the serious, adversarial, hostile and enduring nature of the challenge.[8] It also denotes the ability of a hybrid aggressor to create warlike effects and outcomes (such as disrupting critical infrastructure or even territorial expansion) by 'weaponizing' non-military means, and the possibility that hybrid warfare may be employed to set the conditions to make future conventional aggression more effective.[9] More broadly, it also suggests competitors and adversaries may take a less restricted view of what constitutes 'warfare' and the ways and means deployed to achieve political goals.

In reality, hybrid warfare takes place on a continuum of competition and conflict between actors on the international stage.[10] The challenge for those forming policy and strategy to counter hybrid warfare is to establish where on this continuum the threat of hybrid attack is located and what to do about it. So while it remains useful to understand hybrid warfare as a unified concept, actions taken to counter hybrid warfare must be calibrated to the specific nature, type, and degree of threat or attack. This handbook is designed to provide guidance for this task.

8 MCDC, (2017), Information Note, *What is Hybrid Warfare?* sets out the wider understanding which forms the baseline assessment for this handbook (see Chapter 3).

9 Where 'conventional aggression' refers to international or non-international armed conflict in accordance with the 1949 Geneva Conventions.

10 In this sense, 'hybrid warfare' as described by CHW1 includes concepts such as 'hybrid threats' (see the European Union's 2016 *Joint Framework on Countering Hybrid Threats*, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018), 'gray zone' (see Mazarr, Michael, (2015), *Mastering the Gray Zone: Understanding a Changing Era of Conflict*, available at https://ssi.armywarcollege.edu/pdffiles/PUB1303.pdf) and 'hybrid warfare' (see Frank G. Hoffman, (2009), *Hybrid Warfare and Challenges*, available at http://smallwarsjournal.com/documents/jfqhoffman.pdf).

Why counter hybrid warfare?

The challenge and disruptive potential of hybrid warfare was outlined in CHW1. There are also good reasons to expect an increase in the use of hybrid warfare in the future based on trends in power, interdependence and technology.[11]

- The shifting balance and diffusion of power will mean more actors may be more motivated to challenge the *status quo*.
- With increasing interdependence between actors in the international system, more actors may be increasingly vulnerable to others in more ways.[12]
- Technological development will mean more actors may have more effective and immediate means available to influence and threaten others.

Taken together, these trends are converging to provide revisionist actors with opportunities to seek gains while neutralizing the conventional political or military strength of *status quo* actors. The coming decades may therefore see competition and conflict intensify through hybrid warfare.

On the global and regional levels, rising powers and dissatisfied actors may seek to compete in areas where they can pursue relative advantage. For example, as established powers pursue military superiority, their challengers may further develop hybrid warfare techniques through combining a wider variety of non-military means employed through a wider range of actors to target societal functions in new ways.[13] Hybrid warfare may also be useful to revisionist actors not only as an efficient way to circumvent conventional power, but as an end in itself to subvert and degrade rules and norms.

Hybrid aggressors can be emboldened by the success of carefully-calibrated hostile activity that avoids crossing *de facto* thresholds of decisive response, including through policies of 'plausible deniability'. While such gains may be dismissed as short-term, they leave indelible marks and create dangerous precedents. The potential for hybrid warfare to create destabilizing effects in the international system requires a strategic response.

11 For further detail see UK Ministry of Defence, (2018), *Global Strategic Trends – The Future Starts Today*, page 125-147, available at https://www.gov.uk/government/publications/global-strategic-trends

12 Keohane, Robert and Nye, Joseph S., (1998), *Power and Interdependence in the Information Age*, Foreign Affairs, September/October 1998, 77, page 5.

13 MCDC, (2019), Research paper, *Hybrid War and Its Countermeasures: A Critique of the Literature*, page 145. See Annex A.

Setting strategic goals for countering hybrid warfare

The first step in countering hybrid warfare is to identify the threat. The CHW1 Analytical Framework described the difficulties of establishing hybrid warfare situational awareness. Chapter 3 of this handbook takes this further by exploring new conceptual approaches, based on specific case studies, to inform the development of warning intelligence against hybrid threats and attacks.

Once the threat of hybrid warfare has been recognized, the next step is to decide what to do about it. The level of ambition for countering hybrid warfare will not be the same for every actor. It will depend on context, threat intensity, political appetite and capacity for counteraction. Available policy choices may range from simply absorbing attacks, to deterring aggression, to taking more assertive or retaliatory measures to disrupt and prevent further attacks.

These policy choices are articulated through setting strategic goals. These goals should be established at the start of a counter hybrid warfare campaign and revisited continuously in a dynamic strategic environment. All measures and actions taken to counter hybrid warfare must contribute to achieving one or more goals. Three generic strategic goals have been identified for any actor designing a strategy to counter hybrid warfare.[14]

a. Strategic Goal 1 (SG1): maintain capacity for independent action. The most basic goal is to maintain governmental capacity and capability for independent action. As well as combatting the effects of hybrid warfare on the basic functioning of government and society, this goal is also a pre-condition for any subsequent goals. Government and society must build resilience against hybrid threats by evaluating vulnerabilities and establishing a common and coordinated approach to addressing them through a wide range of tools.

b. Strategic Goal 2 (SG2): dissuade or deter an adversary from hybrid aggression. A second, more demanding goal is to dissuade or deter an adversary from conducting hybrid warfare. While actions to maintain the capacity for independent action may have deterrent effect (through deterrence-by-denial), comprehensive deterrence requires going beyond resilience to threaten or impose costs (deterrence-by-punishment). Hybrid deterrence should be established from the outset and re-established if it fails, with thresholds set taking into account the defenders' interests and the adversary's intent and capability. More detail on deterring hybrid actors is set out in Chapter 4.

14 Based on MCDC, (2019), Research paper, *Strategic Goals of Counter-Hybrid Strategies*. See Annex A.

c. Strategic Goal 3 (SG3): disrupt or prevent an adversary from taking further hybrid aggression. The third and most demanding goal is to prevent an adversary from further hybrid aggression. This goal moves beyond deterrence towards measures that will disrupt and degrade an adversary's capacity for action (although these measures possess deterrent value in their own right). This goal is required because a hybrid aggressor may be unlikely to change their behaviour without retaliation designed to degrade their ability or will to carry out hybrid aggression.[15] More detail on measures to respond to hybrid threats or attacks is set out in Chapter 5.

There are a number of principles to consider when setting strategic goals. These are detailed below.

a. Level of goal-setting. Goals should be set at the governmental and multinational level, for the problem of hybrid warfare may only be solved in the strategic and political level through a comprehensive approach.[16]

b. Reinforcing the rules-based international order. Setting goals and taking actions to counter hybrid warfare should reinforce the rules-based international order and strengthen the seams in liberal-democratic societies exploited by hybrid actors. To retain capacity for action, states should avoid tactical or short-term activity that might harm or undermine the rules and norms that stabilize the strategic environment.

c. The consequences of success. If a perfect formula for countering hybrid warfare were to be found, hostile actors that remain motivated may seek alternative or more dangerous ways to demonstrate their grievance. Even setting the threshold for responding to hybrid attacks too low may create a tense and hostile strategic environment in which miscalculation, misperception and escalation become more likely.

d. Surprise is inevitable. In setting goals states must be ready for shocks, surprises, adaptation and innovation by competitors and adversaries who will always seek to be one step ahead.[17] Hybrid attacks

15 MCDC, (2019), Information Note, *Deterrence by Punishment as a way of Countering Hybrid Threats: Why we need to go 'beyond resilience' in the gray zone*. See Annex A.

16 See MCDC, (2017), *Understanding Hybrid Warfare*. For detail on the importance of the strategic and political level see MCDC, (2018), Research paper, *Hybrid War and Its Countermeasures: A Critique of the Literature*, page 144. See Annex A.

17 MCDC, (2018), Information Note, C*an hybrid attacks be deterred? And if so, how do we do it?*

rarely follow a template, so goals and strategies must be reviewed and amended accordingly. More detail on how to deal with 'unknowns' can be found in Chapter 3.

Setting thresholds

The second step is to set thresholds to guide decision-makers in considering when to take specific action to counter hybrid warfare. Thresholds are central to setting strategic goals for two main reasons.

First, as governments cannot respond to every individual incident of hybrid warfare, thresholds must be set according to what level of hostility can be reasonably tolerated and what level requires countering. While thresholds can be tailored across PMESII domains – depending on their criticality or vulnerability to the state in question – the synergistic nature of hybrid warfare requires the threat picture to be examined as a whole, rather than by domain. Figure 2.1 below demonstrates this concept using the CHW1 Framework. Thresholds for detecting hybrid warfare are more complex as they must allow for 'unknown-unknowns', which precludes setting conventional thresholds – this problem is discussed further in Chapter 3.

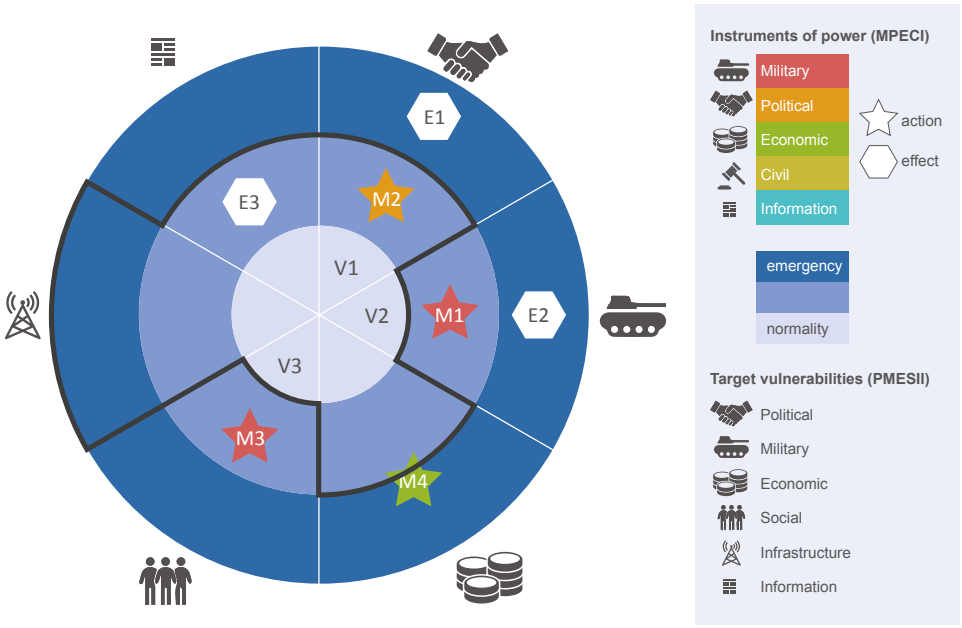


Figure 2.1 – Setting tailored thresholds for countering hybrid warfare

Second, hybrid aggressors purposefully target their adversaries by operating below known or perceived response thresholds to avoid decisive retaliation. Great care should therefore be taken over communicating response thresholds to hybrid aggression or provocation – including how or whether they are communicated, and the consequences of not sticking to them.[18]

Countering Hybrid Warfare Framework

If the strategic goals are the 'ends' of an overall strategy to counter hybrid warfare, then the 'ways' and 'means' required to achieve them are represented by the following three components of the Countering Hybrid Warfare Framework – as shown in Figure 2.2.

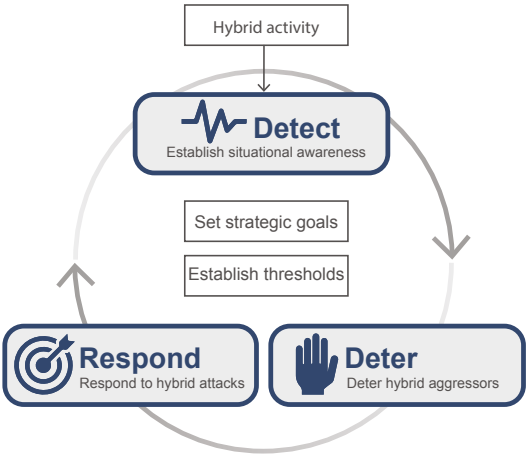


Figure 2.2 – Visualizing the Countering Hybrid Warfare Framework

a. Detect. This component addresses the problem of detecting hybrid threats or attacks in the first place. The Analytical Framework described why hybrid threats may be difficult to detect and how a traditional enemy-centric threat analysis is inadequate for doing so.[19] Chapter 3 describes alternative methods for establishing hybrid warfare situational awareness. The knowledge established through these techniques forms the foundations on which to build a comprehensive strategy to counter hybrid warfare.

18 Communicating deterrence thresholds is covered in more detail in Chapter 4.
19 MCDC, (2017), *Understanding Hybrid Warfare*, page 10.

b. Deter. This component addresses the deterrence of hybrid actors, or 'hybrid deterrence'.[20] Chapter 4 examines the challenges to deterrence posed by hybrid warfare and offers five key principles for deterring hybrid aggressors.

c. Respond. This component addresses how to respond to hybrid threats or attacks. The decision to respond by implementing appropriate actions and measures can be taken at any stage in the hybrid threat cycle, from the identification of potential vulnerabilities that require resilience-building activity to measures taken in response to a specific hybrid attack. Chapter 5 examines the challenge of responding to hybrid threats or attacks and offers a framework for making decisions about doing so.

Key points

- Hybrid warfare represents a serious, disruptive and enduring challenge to the international system. It takes place on a continuum of competition and conflict between international actors. Countering it requires strategic approach.
- Once the threat of hybrid warfare has been identified, the first step is to set the level of ambition for countering it. This is captured through setting one or more strategic goals (SG).

  SG1: maintain capacity for independent action.
  SG2: dissuade or deter an adversary from hybrid aggression.
  SG3: disrupt or prevent an adversary from taking further hybrid aggression.

- The second step is to set thresholds to guide decision-makers in considering when to take specific action to counter hybrid warfare.
- A strategy to counter hybrid warfare must then be designed, implemented and reiterated, based on three components.

  Detect hybrid warfare.
  Deter hybrid aggressors.
  Respond to hybrid attack.

20 As opposed to 'conventional deterrence'.

> One way to consider warning intelligence for hybrid warfare is to differentiate potential future hybrid attacks into two separate categories of ‘known unknowns’ and ’unknown unknowns’.

Chapter 3

Detecting hybrid warfare

This chapter addresses the problem of detecting hybrid warfare so action can be taken to counter it. Building on the CHW1 Analytical Framework that described why hybrid threats are difficult to detect and why a traditional enemy-centric threat analysis is inadequate for doing so,[21] this chapter describes alternative methods for establishing hybrid warfare situational awareness. It does so by first discussing the challenges hybrid warfare creates for traditional, military-centric indicator-based early warning and detection, followed by a basic typology of methods for detecting hybrid warfare. It also summarizes four case studies to provide insights about how to do this in practice.

Warning intelligence

Warning intelligence refers to intelligence activities that detect and report time-sensitive developments that forewarn of hostile actions or intent. It traditionally relies on indicator-based methods, where key indicators are identified and monitored over time to establish a baseline of an adversary's 'normal' activities and operations. Indicator-based warning intelligence is focused on detecting relevant changes in operational status that can provide intelligence analysts and decision-makers with an alert – or early warning – of undesirable activity.

> For various reasons, some obvious and some less well-recognized, the collection and analysis of military data or indications is the predominant element in warning. By far the greater number of items or indicator lists deal with military, or military-related, activities. By far the greater portion of the collection effort, and particularly the most expensive collection, is devoted to obtaining data on the military strengths, capabilities and activities of enemy and potential enemy forces.
>
> Cynthia Grabo[22]

21 MCDC, (2017), *Understanding Hybrid Warfare*, page 10. See also Dr Patrick Cullen (NUPI), (2018), *Hybrid threats as a new 'wicked problem' for early warning*, available at https://www.hybridcoe.fi/wp-content/uploads/2018/06/Strategic-Analysis-2018-5-Cullen.pdf

22 Grabo, Cynthia, (2015), *Handbook of Warning Intelligence*, Rowman and Littlefield (complete and declassified edition), page 113.

The quote from Cynthia Grabo illustrates the traditional focus in warning intelligence on military capabilities and activities. Yet this approach is inadequate when it comes to an adversary that employs hybrid warfare. While military and traditional indicators remain important, the challenge of detecting hybrid warfare requires moving beyond this one-dimensional approach to warning intelligence by expanding what traditionally has been considered relevant to watch.

The emphasis in hybrid warfare on creating and exploiting ambiguity and deception, combined with creatively using non-military tools to target all areas of society, requires the creation of warning intelligence processes and methods aimed at protecting critical vulnerabilities across society from attack. Detecting synchronized, multi-vector hybrid attacks intentionally designed to fall outside and or below traditional detection thresholds will also require coordinated information sharing.

As will be demonstrated below, the challenge posed by hybrid warfare cannot simply be addressed by developing new indicators. Since the potential ways and means of hybrid attacks are difficult (or impossible) to predict, entirely new approaches to warning intelligence must be produced that move beyond indicator-based methods.

Hybrid warfare early warning and situational awareness

One way to consider warning intelligence for hybrid warfare is to differentiate potential future hybrid attacks into two separate categories of 'known unknowns' and 'unknown unknowns'. Known unknowns refer to modes of hybrid attack that we know we may be unaware of. However, risk related to hybrid attacks may also exist where we are not even aware of its nature, our vulnerability to it, or even of our own ignorance to the threat. This is the field of unknown unknowns. A useful way of developing this concept for hybrid warfare warning intelligence is to differentiate monitoring from discovery.

a. Monitoring involves a process of scanning the environment for known unknowns – usually with the aid of indicators – to look for a set of preconceived information about possible hybrid warfare attacks.

b. Discovery, on the other hand, involves an attempt to manage the problem of unknown unknowns. This process involves capturing and then correctly interpreting information related to a potentially hostile adversarial action that has not been previously conceived. This type of information is not amenable to a monitoring methodology built upon

> 'perceiving what we expect to perceive' via either pattern recognition or the use of indicator lists. This is because the analyst has never seen this pattern before, and cannot be equipped with an indicator list for a type of attack that has never occurred or even been imagined before.

Importantly, the practice of discovering unknown unknowns need not sit in opposition to practices of monitoring *per se*, but does require a different type of monitoring focused on detecting anomalies and developing practical techniques to recognize previously unseen patterns. Figure 3.1 below shows the basic idea of distinguishing between 'monitoring' and 'discovery' in warning intelligence for hybrid warfare.

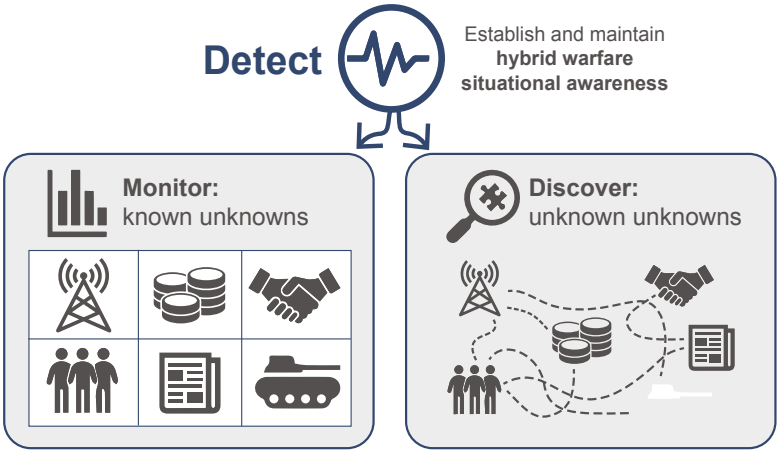


Figure 3.1 – Distinguishing between 'monitoring' and 'discovery' in warning intelligence for hybrid warfare

To demonstrate these ideas in practice, the following four case studies provide an overview of four initiatives to develop early warning for hybrid warfare in both homeland security and deployed contexts. While the first two case studies (Austria and the United States (US)) provide examples of how and why indicator-based methodologies are being expanded to cover a larger set of potential threats, the latter two case studies (Finland and the United Kingdom (UK)) point to alternative warning methodologies that move beyond indicators. Figure 3.2 demonstrates how the case studies map onto the proposed framework.

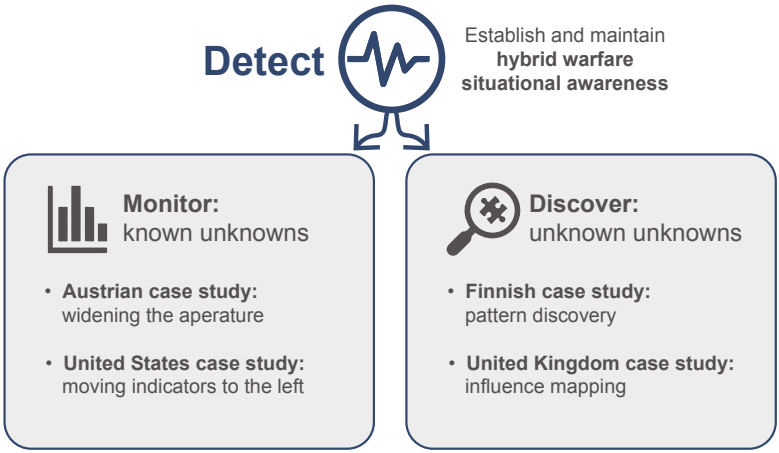


Figure 3.2 – Mapping the four case studies

Hybrid warfare as a known unknown: widening the aperture (Austrian case study)

The Austrian military is currently experimenting with ways to 'widen the aperture' of warning intelligence methods to cope with the wide array of potential threats posed by hybrid warfare. One way they are doing this is to adapt 'centre of gravity' analysis – a widely used but military-centric planning tool. Centre of gravity analysis has the potential to improve hybrid warfare early warning through anticipating the use of unconventional or non-military means of attack across a much wider set of critical vulnerabilities across society. The basic process has four parts. These are:

- identifying national critical vulnerabilities;
- linking them to assumptions or hypotheses of adversary objectives and capabilities;
- developing new warning indicators linking the two; and
- deriving actions, effects and conditions required to counter these threats (in a whole of nation approach).

Crucially, for the centre of gravity methodology to create new indicators of hybrid warfare across all sectors of society it will require the active participation of the civilians with the subject matter expertise from across government (and ideally the private sector) to usefully apply their practical knowledge.

Hybrid warfare as a known unknown: moving indicators to the left (United States case study)

One approach to adapting indicators for hybrid warfare in the US advocates for a 'shift to the left' of hostile-activity indicators on a peace-war spectrum.[23] This approach is related to, but conceptually distinct from, the previous approach of 'widening the aperture' because it is not focused on expanding the monitoring mission to new places *per se*, but is instead focused on expanding the monitoring mission of warning intelligence to include adversarial behaviour falling well below the threshold of conventional conflict. In the words of US Army Special Operations Command (USASOC), there is a need 'to perceive indications of challenges, threats, and opportunities for non-standard campaigns that state and non-state actors are pursuing on the left side of the operational spectrum.'[24]

For USASOC, hybrid warfare creates challenges for warning intelligence precisely because it requires the intelligence analyst to create and monitor indicators for security challenges that were previously considered too minor or insignificant to even be considered relevant, or too under-developed to be monitored. Elements of the US special operations community have argued that the need for developing new 'gray zone' or hybrid warfare indicators creates an intelligence collection requirement – and one that special operators are uniquely capable of fulfilling for the intelligence community. For example, the collection of ambiguous 'human domain' data (such as population-centric information about the inhabits of a locale[25]), relevant for strategic warning that is not being exploited either because it falls below or outside of traditional collection thresholds for operational warning intelligence, or because the human intelligence resources were not available.[26] In particular, the US special operations community see themselves in a position to leverage their global deployment footprint to identify subtle early-stage indications of hybrid warfare operations.

23 See for example, Hoffman, Frank G., (2016), *The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War*, Heritage Foundation, Figure 1, page 29, available at https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_ESSAYS_HOFFMAN.pdf

24 US Army Special Operations Command, (2016), *Perceiving Gray Zone Indications*, page 1, available at https://www.soc.mil/Files/PerceivingGrayZoneIndicationsWP.pdf

25 For more on the human domain, see US Army Special Operations Command, (2015), *Operating in the Human Domain*, available at https://nsiteam.com/social/wp-content/uploads/2017/01/SOF-OHD-Concept-V1.0-3-Aug-15.pdf

26 US Army Special Operations Command, (2016), *Perceiving Gray Zone Indications*, page 1.

Hybrid warfare as an unknown unknown: pattern discovery (Finnish case study)

The two previous case studies have looked at attempts to update and adapt the use of indicator-based warning to hybrid warfare. This case study shifts the focus to some experimental work being conducted by the Finnish government on alternative methods for 'discovering' the harder to detect 'unknown unknown' hybrid threats. Here, analysts work on pattern discovery, the identification of new patterns. In a shift from the reliance upon indicators, this approach focuses on the detection of anomalies or clues of possible ambiguous hybrid threats. Through placing a handful of analysts in the Prime Minister's office, an effort is made to reach out horizontally to ministries, and other governmental and private entities, to report on all incidents of an unusual nature, regardless of its apparent insignificance.

This approach represents an attempt to discover and map ambiguous activities that potentially provide early weak signals of a developing hybrid threat that normally would never be put together by any intelligence or domestic, counter-intelligence agency. Moreover, the method aims to break down informational stovepipes between government agencies and the private sector to help analysts develop greater situational awareness, genuinely representing a national effort to combine information that can lead to discovery of events of potential hybrid character. The Finnish approach also involves bureaucratically elevating a 'hybrid analysis unit' into the Prime Minister's office to allow rapid warning of hybrid threats if required.

Hybrid warfare as an unknown unknown: influence mapping (United Kingdom case study)

Another example of a creative experimental method to discover potential hybrid threats is the 'hybrid activity monitoring tool', developed by the UK Ministry of Defence. This tool is designed to help identify potential hybrid activity through open source information and enable decision-makers to better understand the events as they take place. This method is designed to support decision-making in an uncertain hybrid threat environment through seeking to understand what hybrid activity is happening, and what 'levers' of power might be used. The original 'levers' selected were: infrastructure; political; economic; social; military; and media/information.

Each lever is graded against two dimensions: level of influence; and impact of influence. By reporting incidents in this way, a total score can be calculated by multiplying the two dimensions together. By defining specific criteria to look for, and comparing collected information with an established 'normal' baseline, a graphic visualisation of the potential hybrid activity level can also be produced.

Lessons for hybrid warfare early warning

Hybrid warfare challenges the traditional use of indicator-based methods for early warning of hostile intent and activity focused on the military domain. Efforts to develop early warning against hybrid warfare should instead focus on both expanding indicator-based monitoring methods, and creating new approaches to discovering ambiguous or hidden hybrid threats by finding and filtering unanticipated anomalies.

Four case studies provide insights about how to do this in practice.

a. The Austrian example demonstrates that the creative re-imagining of indicator-based warning is crucial for responding to the challenges posed by hybrid warfare's coordinated use of economic, informational and other non-military tools of statecraft against targets across the whole of society.

b. The US case study demonstrates that since hybrid warfare is tailored to operate in a 'gray zone' that falls short of, or outside of, our traditional understanding of 'warfare', new warning indicators should be developed to fill this gap.

c. The latter two case studies – focused on Finnish and UK approaches to hybrid warfare early warning – point to alternative warning methodologies that move beyond indicators. They each demonstrate creative approaches to 'discovering' ambiguous or hidden threats generated from 'unknown unknowns' by finding unanticipated anomalies from a given norm, rather than from watching for changes to a preconceived list of indicators.

Future efforts to provide early warning against hybrid warfare should develop and experiment with a combination of these approaches.

Key points

- Hybrid warfare challenges the traditional use of indicator-based methods for early warning of hostile intent and activity in specific domains.

- Since the potential ways and means of hybrid attacks are difficult (or impossible) to predict, entirely new approaches to warning intelligence must be produced that move beyond indicator-based methods.

- One way to consider warning intelligence for hybrid warfare is to differentiate monitoring from discovery.

  Monitoring involves a process of scanning the environment for 'known unknowns'.

  Discovery deals with 'unknown unknowns' by capturing and interpreting information related to a potentially hostile adversarial action that has not been previously conceived.

- Future efforts to provide early warning against hybrid warfare should develop a combination of these approaches. Experimental efforts are underway in various nations, including Austria, the United States, Finland and the United Kingdom.

Notes

> Where traditional deterrence has often succeeded in dissuading revisionist actors from resorting to conventional armed aggression, it has often failed to dissuade the same actors from conducting hostile activity – in the form of hybrid warfare.

Chapter 4

Deterring hybrid aggressors

Hybrid threats and deterrence

Deterrence is perhaps the most important tool for countering hybrid warfare, simply because it can prevent attacks occurring in the first place. However, the characteristics of hybrid warfare serve to complicate the traditional deterrence calculus. Effective 'hybrid deterrence' therefore requires updating traditional approaches to deter modern hybrid threats. To do so, this chapter examines the basic principles of deterrence, how they are challenged by hybrid warfare and how to address these challenges. A framework is then developed based on five key principles for hybrid deterrence.

Basic principles of deterrence

The nature of deterrence is based on a simple cost-benefit calculation that compares the perceived cost of an action to its potential benefit.[27] Effective deterrence can be understood to rest on the following three pillars – or the 'three Cs' of deterrence.

- Credibility is the will to carry out actions that impose costs on the adversary.
- Capability is the ability or technical capacity to carry out actions that impose costs on the adversary.
- Communication is the two-way understanding and perception that informs cost-benefit calculations on both sides.

Deterrence strategies come in two broad categories. These are deterrence by denial and deterrence by punishment.[28]

- Deterrence by denial aims to undermine the ability of the adversary to achieve their objective in the first instance.

27 However, the outcome remains context-specific and will depend on many factors. For example, motivation, capability, intent, perception and the 'rationality' of decision-makers.

28 This distinction was originally made in Glenn H. Snyder, *Deterrence and Defense*, Princeton University Press, 1961.

- Deterrence by punishment aims to persuade the adversary the costs of achieving their objective will be prohibitive by threatening retaliation to aggressive action.

Deterrence and hybrid warfare

Hybrid warfare complicates and challenges the logic of deterrence described above. The problem of deterring an actor who employs hybrid warfare can be demonstrated by analyzing the three 'pillars' of deterrence against the three main characteristics of hybrid warfare developed in the CHW1 Analytical Framework. This is shown in Table 4.1.

Hybrid warfare characteristics*	The 'three pillars' of deterrence		
	Credibility	Capability	Communication
The combined use of multiple instruments of power to achieve asymmetry through targeting an expanded range of vulnerabilities.	Credible options for retaliation are undermined or removed by avoiding detection in the first place and exploiting asymmetry in risk appetite.	It is challenging to map and address a wide range of potential vulnerabilities, and difficult to achieve a coherent response to a varied and unconventional attack.	It is difficult for the target of hybrid warfare to detect and understand the occurrence of and intent behind low-level and disconnected activity.
A multi-modal and synchronized attack along both horizontal and vertical axes of escalation.	The defender is overwhelmed by attacks on multiple fronts. Attacks tailored to remain below response thresholds undermine the defender's will and ability to respond.	Traditional tools of statecraft (for example, diplomacy and military) are designed to respond to discrete threats.	Horizontal and vertical escalation complicates setting and communicating response thresholds, and undermines conventional decision-making systems. It is also difficult to map and predict cause and effect, and therefore communicate risk (for example, to the population).
An emphasis on creativity, ambiguity and effects in the cognitive domain. * Characteristics taken from MCDC, (2017), *Understanding Hybrid Warfare*, page 15.	Tenets of hybrid warfare such as gradualism, ambiguity, deniability and deception deny the conditions required to take decisive counteraction. Ambiguity can undermine the defender's resolve to respond as it is difficult to justify responding to actions that are seemingly trivial or unattributed. Hybrid aggressors often seek to undermine collective deterrence and societal resilience by exploiting division.	Hybrid warfare tests the ability of the defending actor to respond to creative and unpredictable attacks. Societal resilience is less of a technical capability challenge and more political – which is difficult to counter with concrete actions.	Hybrid warfare undermines communication and shared understanding between actors through ambiguity, asymmetry (in risk appetite or ethical standards), attribution, deception and increased noise. As new patterns of hostile activity and response thresholds are established, the potential for miscalculation is high on both sides.

Table 4.1 – How the main characteristics of hybrid warfare affect the three pillars of deterrence

Modern deterrence theory

The problem of deterring hybrid warfare actors – or 'hybrid deterrence' – can be seen as part of the broader challenge of deterrence in the 21st Century. Developments in deterrence theory since the turn of the century may therefore be applied to deterring hybrid aggressors. These include the so-called 'fourth wave' of deterrence theory, and more recent developments in cyber deterrence.[29]

a. Fourth wave deterrence theory is characterized by two key elements that are relevant to hybrid warfare. First, a shift away from the relatively symmetrical mutual deterrence of state-actors towards deterring 'asymmetric' threats from non-state and pseudo-state actors. Second, the recognition of a broader concept of deterrence that goes beyond military means.[30]

b. The field of cyber deterrence overlaps with hybrid deterrence in terms of both context and the basic challenge. The context involves applying non-military technological means to achieve influence and threaten harm. The basic challenge is one of attribution difficulty, asymmetry, psychology, vulnerability, ambiguous response thresholds and an uncertain retaliation calculus.[31]

In the countering hybrid warfare project, the developments in deterrence theory outlined above were applied to the problem of deterring hybrid aggressors through research papers and workshops.[32] In the next section the insights from this work are incorporated into a framework and set of principles for deterring hybrid aggressors – thereby achieving Strategic Goal 2 – dissuade or deter an adversary from hybrid aggression.

29 There is also a nascent literature on so-called 'gray zone' deterrence. See for example Mazarr, Michael, (2015), *Mastering the Gray Zone: Understanding a Changing Era of Conflict*; CSIS, (2018), *What Works: Countering Gray Zone Coercion,* available online at https://www.csis.org/analysis/what-works-countering-gray-zone-coercion; or Takahashi, Sugio, (2019), *Development of gray-zone deterrence: concept building and lessons from Japan's experience*, The Pacific Review.

30 For the original 'waves' characterisation see Jervis, Robert, (1979), *Deterrence theory revisited*, World Politics 31.2, pages 289-324. For more on 'fourth wave' see Knopf, Jeffrey W., (2010), *The fourth wave in deterrence research,* Contemporary Security Policy 31.1, pages 1-33.

31 See Andres, Richard, (2017), *Cyber Gray Space Deterrence*, PRISM, volume 7, No. 2, pages 91-98.

32 See MCDC Information Notes: *Can hybrid threats be deterred? And if so, how do we do it?; Hybrid Warfare: Understanding Deterrence; and Deterrence by Punishment as a way of Countering Hybrid Threats: Why we need to go 'beyond resilience' in the gray zone.* Also see MCDC research papers: *Hybrid Warfare and Deterrence*; and *Gray Zone Concept: Competition Short of Armed Conflict*. See Annex A for further details.

A framework for hybrid deterrence

> The theories of deterrence remain applicable...but strategists must determine whom to deter, how to deter them, when, and why.

Colin S. Gray[33]

This section describes a framework for designing a strategy to deter aggressors who use hybrid warfare – 'hybrid deterrence'. This is summarized in Figure 4.1.. However, as Colin S. Gray observes, the fundamental problem of deterrence remains one of practice, not theory, so may only be solved based on a sophisticated understanding of whom, how, when and why. There are no shortcuts or 'magic recipes' for deterring aggressors, no matter what form they take.

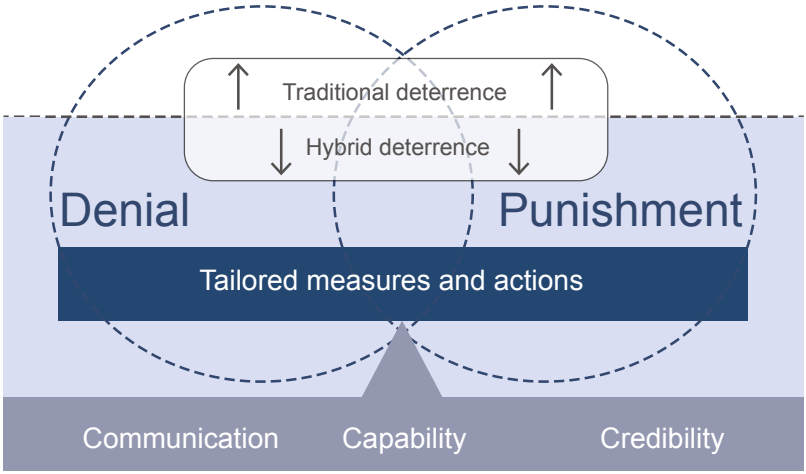


Figure 4.1 – A hybrid deterrence framework

33 Gray, Colin S., (2000), *Deterrence in the 21st century*, Comparative Strategy, Volume 19, Issue 3.

Key principles for deterring hybrid aggressors

The framework summarized in Figure 4.1 reflects five key principles for deterring hybrid aggressors. These are detailed in Infobox 4.1.

Infobox 4.1 – Five key principles for deterring hybrid aggressors

1) Traditional deterrence remains vital. It both dissuades armed aggression (above the dotted line) and contributes to deterring hybrid attacks (below the dotted line).

2) Hybrid aggressors are deterrable. Revisionist actors can be specifically deterred from using hybrid warfare – through 'hybrid deterrence'.

3) The 'three Cs' of deterrence look different through a hybrid lens. The characteristics of hybrid warfare place specific demands on the 'three Cs'.

4) Resilience is important – but not enough to change behaviours. Hybrid deterrence requires a balance between deterrence by denial and deterrence by punishment.

5) Pursue a tailored approach to deterrence. Deterrence measures must be tailored to the aggressor and situation.

Principle 1 – Traditional deterrence remains vital

The rise of hybrid warfare can be traced to both successes and failures of traditional deterrence. Where traditional deterrence has often succeeded in dissuading revisionist actors from resorting to conventional armed aggression, it has often failed to dissuade the same actors from conducting hostile activity – in the form of hybrid warfare.[34]

Traditional deterrence policies should therefore be maintained – and even strengthened – to continue to deter motivated revisionist actors from resorting to armed aggression. Traditional deterrence also contributes to deterring hybrid attacks, making a hybrid aggressor think twice where the threshold for response to such aggression is uncertain.

34 The phrase 'traditional deterrence' is used to refer to deterrence through conventional, nuclear and 'modern' means (such as cyber).

However, the potential damage to society and risk of continuous 'low-level' hybrid attacks require addressing the shortfalls of traditional deterrence in deterring hybrid attacks. The next four principles therefore consider how to deter aggressors from conducting hybrid attacks more specifically.[35]

Principle 2 – Hybrid aggressors are deterrable

Traditional deterrence measures should be complemented by specific measures to deter hybrid aggressors. While the characteristics of hybrid warfare may complicate deterrence, the difficulties should not be overstated for four main reasons.[36]

a. Hybrid attacks involve the pursuit of interests by actors within a specific context. This allows adversary intent and capability to be discerned to some degree.

b. Although hybrid warfare exploits ambiguity, the specific means used by aggressors are often attributable. The attribution challenge is often primarily a political one, rather than a technical one.[37]

c. Deterring actors are rarely powerless, even in the face of ambiguity and uncertainty. For example, preparatory actions such as addressing potential vulnerabilities through resilience measures are often low-cost.

d. Hybrid aggressors are vulnerable too. Their weaknesses can be exploited through more assertive responses that creatively combine vertical and horizontal escalation. Hybrid aggression may also be a sign of weakness in itself – towards conventional military, political and normative power.

35 In doing so, the consequences of successful hybrid deterrence should be carefully considered, for hostile actors that remain motivated may seek alternative or more dangerous ways to demonstrate grievances.

36 MCDC, (2018), Information Note, C*an hybrid attacks be deterred? And if so, how do we do it?*

37 This point was brought out during the MCDC CHW table top exercise (see Annex D). Actors did not pursue attribution more often due to the political consequences of doing so, rather than the technical inability to do so.

Principle 3 – The 'three Cs' of deterrence look different through a hybrid lens

Effective deterrence of hybrid aggressors still rests on the 'three Cs' of deterrence (page 35), but these should be interpreted differently in the context of hybrid warfare.

a. Credibility. Protect and create credible deterrence options by pursuing the following actions.

- Develop numerous creative, low-level horizontal retaliation options across the MPECI levers of power that are politically achievable but demonstrate clear resolve.
- Bolster the enablers of deterrence action, such as public threat awareness.
- Prepare for collective deterrence and multinational action through institutional arrangements in anticipation of hybrid attack.
- Set clear thresholds for response and stick to them – ensure consistency of rhetoric and actions, but also consider taking opportunities to be unpredictable towards the aggressor (see 'Communication' below).

b. Capability. Develop the tools, techniques and procedures to detect a wider range of potential hybrid threats, with more confidence, earlier. Enhance and expand the range of tools available to both address vulnerabilities and prosecute deterrence measures targeted towards the aggressor, by exploiting both vertical and horizontal escalation. Develop the coordination mechanisms and culture required to take a comprehensive, whole-of-government and multinational approach to hybrid deterrence policy (see Chapter 6).

c. Communication. Establish clear and realistic thresholds for deterrence and response. Set too low these will be untenable and potentially counter-productive (not all hybrid threats can be deterred at all times); set too high they may encourage aggression. Consider the effects of communicating thresholds clearly against maintaining constructive ambiguity. Well-signposted thresholds can avoid miscalculation but the knowledge of 'red lines' can encourage

aggression just below them. Hidden or vague thresholds may deter through unpredictability, but can also invite miscalculation. Bear in mind that all actions communicate something to someone. The key to successful strategic communications is to understand the audience, understand and exploit the information environment, and integrate words and actions across government.[38]

Principle 4 – Resilience is important – but not enough to change behaviours

Research for this project has shown it is unlikely that resilience measures on their own will change the behaviour of a hybrid aggressor.[39] Therefore, if the strategic goals of the defending actor include deterring further hybrid attacks (SG2), an appropriate balance must be struck between deterrence by denial and punishment measures. Infobox 4.2 (page 44) discusses how to update traditional ideas about doing this.

A revitalized deterrence by punishment strategy towards hybrid aggressors relies on identifying and communicating credible punitive actions across a wider-spectrum of non-military means tailored towards key PMESII vulnerabilities of the aggressor. Chapter 5 discusses illustrative ways and means for doing this. Such an approach is the basis of a proportionate and legitimate response to 'non-violent' aggression.[40] Deterrence measures should also be complemented with inducement and reassurance actions to reinforce 'off-ramps' away from aggression and escalation.[41]

The balance of resources invested into deterrence measures will be a matter for each nation. As a general rule, spending across different sectors (for example, whether on public education, infrastructure resilience or high-end military capability) will not only bolster deterrence by denial – such as through societal resilience – but also contribute positively to overall deterrence.

38 NATO Strategic Communications Centre of Excellence (2019), *Hybrid Threats: A Strategic Communications Perspective.*

39 MCDC, (2019), Information Note, *Deterrence by Punishment as a way of Countering Hybrid Threats: Why we need to go 'beyond resilience' in the gray zone*. See Annex A for information note with further detail in Annex C.

40 See MCDC, (2019), Information Note, *Deterrence by Punishment as a way of Countering Hybrid Threats: Why we need to go 'beyond resilience' in the gray zone*. See also Sari, Aurel, (2019), 'Hybrid Warfare, Law and the Fulda Gap', in Christopher Ford and Winston Williams (eds), *Complex Battle Spaces*. This argument is also made in Allen, Duncan, (2018), *Managed Confrontation: UK Policy Towards Russia After the Salisbury Attack*, Chatham House.

41 Jakobsen P.V., (1998), Constructing a Theoretical Framework; Chapter 3 in *Western Use of Coercive Diplomacy after the Cold War*, Palgrave Macmillan, London.

Infobox 4.2 – Modern deterrence and hybrid warfare

Considering how to update traditional ideas about deterrence can help inform effective modern hybrid deterrence, which requires an appropriate balance between measures to support.

- Deterrence by denial: modernizing 'total defence'. A key component of denial for hybrid deterrence is increasing resilience by addressing vulnerabilities across government and society. There are numerous recent examples of modern whole-of-society approaches to resilience in the 21st Century.[42] The next section (page 45) discusses illustrative ways and means of doing this.

- Deterrence by punishment: modernizing 'flexible response'. To be effective, punishment strategies require a renewed approach to flexibly exploiting horizontal escalation across the MPECI levers of power, targeted towards PMESII vulnerabilities. Chapter 5 discusses illustrative ways and means of doing this.

Principle 5 – Pursue a tailored approach to deterrence

Hybrid deterrence is ultimately about marginal gains through tailored deterrence. Research in this project has suggested that a logical, actor-centric approach that disaggregates the concept of hybrid warfare and considers marginal gains has potentially vast utility.[43] There are five ways to tailor an approach to deterring hybrid aggressors.

a. Disaggregate the strategy of any 'hybrid' adversary. This enables the construction of a tailored deterrence strategy that targets specific elements of the overall campaign. In other words, rather than aim to deter hybrid aggression as a whole, consider a disaggregated version of hybrid warfare as a collection of complementary strategies.

b. Seek marginal gains. Just as the power of hybrid warfare stems from the cumulative effect of coordinated actions, any approach to

42 Examples – Sweden ('Total Defence'), Norway ('Support and Cooperation'), Finland ('Comprehensive Security'), Austria ('Comprehensive National Defence') and Singapore ('Total Defence').

43 See MCDC, (2019), Information Note, *Hybrid Warfare: Understanding Deterrence* and MCDC, (2019), Research paper, *Hybrid Warfare and Deterrence.* The following principles are supported by historical and contemporary case studies conducted throughout the project which have considered deterrence of hybrid state and non-state actors. See Annex A.

deterring them must consider how to tip the balance through small steps. Rather than focus on total or comprehensive deterrence, against complex, gradualist hybrid threats, the most viable approach is through marginal gains and focused targeting of key vulnerabilities (of both the defending actor and the hybrid aggressor).

c. Target specific assets that are key to enabling a hybrid campaign. For example, hybrid actors value the use of informational means to sow doubt and confusion, but these can be targeted or threatened in specific ways (through attribution, obstruction and counter-narratives).

d. Think performatively about the best means to deter. A hybrid deterrence posture may be built around the most credible means (the most efficient, or the most viable) rather than the most threatening means.

e. Increased focus on actors. Understanding actors remains central to deterrence. Hybrid actors still have goals, motivations and vulnerabilities that can be discerned and exploited to inform a deterrence strategy. The more an actor can be understood, the more tailored and effective deterrence measures will be.

Ways and means for deterring hybrid aggressors

This section considers ways and means for deterring hybrid aggressors by focusing on deterrence by denial against hybrid threats. These measures aim to enhance resilience and minimize the consequences of hybrid attacks by securing PMESII vulnerabilities. Deterrence by punishment is considered in Chapter 5, as the ways and means to respond can be threatened as deterrence by punishment.[44]

Deterrence by denial in the PMESII domains

a. Political. In terms of political preventive means, restricting or prohibiting foreign financing of political parties or party-affiliated political organizations may prevent dependencies of, or influence on, political decision-making processes. To foster societal trust in democratic institutions, electoral processes can be secured. All efforts should be widely communicated.

44 Conceptual development in this project has also shown the importance of inducement to complement deterrence and response measures. This concept is discussed in Chapter 5.

b. Military. Military strength and international defence cooperation remain vital to the credibility of traditional deterrence (by denial and punishment). The military contribution to homeland resilience is fundamental, and should be reconsidered in the light of modern hybrid threats.[45] Furthermore, the resilience of defence itself against hybrid threats is also important (see Chapter 6).

c. Economic. One credible preventive economic measure against hybrid threats is the security and diversity of strategic resources. Raising situational awareness on hybrid threats within private companies is also important.[46] Anti-corruption is vital: corrupt systems weaken resilience, undermine trust and can be exploited by hybrid actors.[47]

d. Social. The exploitation of social division and special interest groups through foreign financing and support should be addressed. Education can enhance situational awareness on the existence and forms of hybrid threats and the actions required by government or by wider society. To maximize resilience, the population must be aware of, and involved in, resilience-building and preparatory measures.[48]

e. Infrastructure. Resilience and preventive measures require both physical and non-physical protection measures. Physical protection includes a range of measures to secure physical, organizational and digital infrastructure, while non-physical measures include legislation, financial transparency and trade regulation.[49]

f. Information. The central proactive element to counter hybrid threats is strategic communication. This can be targeted both inwardly, towards society, and externally, towards aggressors, their societies and the international community. In this context, proactive and transparent cooperation with media (both digital and traditional) is crucial.

45 See MCDC, (2019), Information Note, *A review of UK Defence's contribution to homeland resilience and security in light of the changing global context*. See Annex A.

46 See Helsinki Region Chamber of Commerce, (2018), *Business Community and Hybrid Threats*, available at http://view.24mags.com/mobilev/bbc43250c51aa3c0b599cb18066f3c2b#/page=1

47 MCDC, (2019), Information Note, *'A deadlier peril': The Role of Corruption in Hybrid Warfare.*

48 For example, Sweden published in 2018 the brochure *If War or Crisis comes* (https://www.msb.se/en/Tools/News/The-brochure-If-Crisis-or-War-Comes-is-available-to-download/) and the city of Helsinki the booklet *Helsinki in the era of hybrid threats – Hybrid influencing and the city* (https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti_eng_020818_netti.pdf).

49 Such as the European Program for Critical Infrastructure Protection (EPCIP). Details available at https://ec.europa.eu/home-affairs/content/european-programme-critical-infrastructure-protection-epcip_en

Visualizing hybrid deterrence

Figures 4.2 and 4.3 below demonstrate a way of visualizing a strategy to deter hybrid aggressors, building on the concepts from CHW1 but with some key changes. Here, the thresholds represent the strategic goal of each measure, while the background indicates whether the defender's or aggressor's vulnerabilities are being targeted.

a. Figure 4.2 shows a mixture of deterrence by denial measures aimed at achieving Strategic Goal 1 and Strategic Goal 2. These measures are activated according to the thresholds for action, and are aimed at addressing the defender's vulnerabilities.

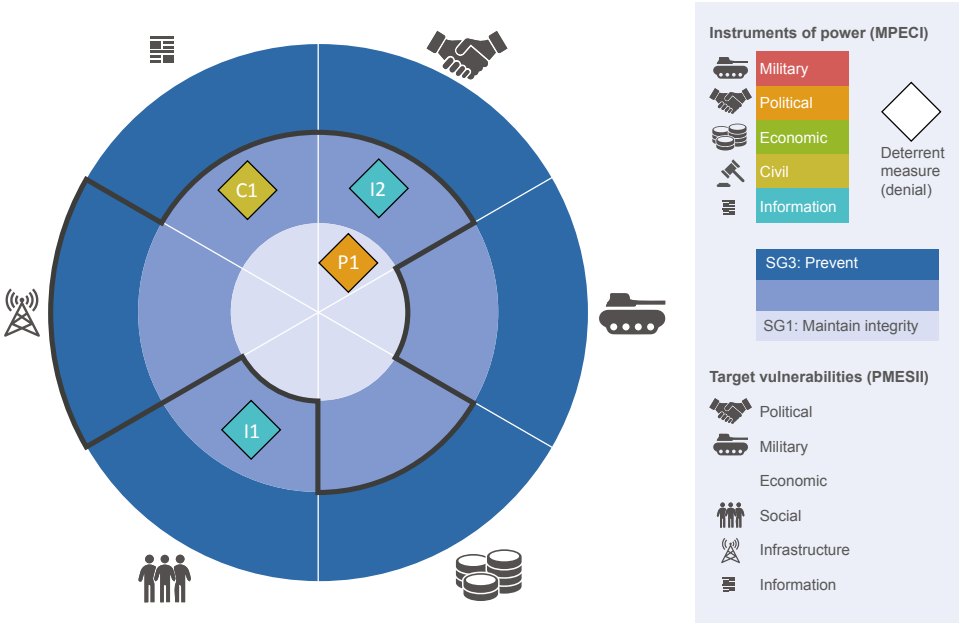


Figure 4.2 – Visualizing deterrence by denial measures (targeted as addressing the defender's vulnerabilities)

b. Figure 4.3 shows a mixture of deterrence by punishment measures aimed at achieving Strategic Goal 2. The graphic is a different colour because these measures are targeted at the aggressor's vulnerabilities, and threatened as punishment should a given threshold of hostility be crossed.

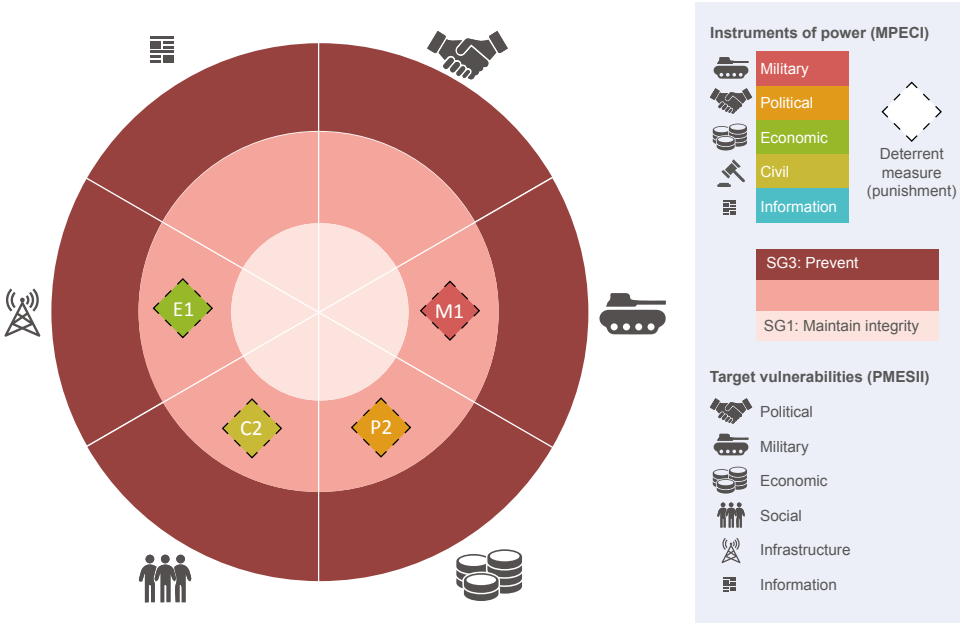


Figure 4.3 – Visualizing deterrence by punishment measures (targeted at the aggressor's vulnerabilities)

Key points

- Hybrid warfare complicates and challenges the traditional logic of deterrence across the 'three Cs' of credibility, capability and communication.
- The problem of deterring aggressors who use hybrid warfare – or 'hybrid deterrence' – can be seen as part of the broader challenge of modern deterrence in the 21st Century.
- Deterring hybrid aggressors can be done, but it requires building on traditional deterrence to pursue credible measures through creative horizontal escalation, tailored and communicated to the aggressor, that are balanced between deterrence by denial – or resilience – and punishment.
- Deterrence by denial measures achieve Strategic Goal 1 and Strategic Goal 2 through enhancing the resilience of government and society, minimizing the consequences of hybrid attacks by securing PMESII vulnerabilities. These measures are activated according to the thresholds for action, and are aimed at addressing the defender's vulnerabilities.
- Deterrence by punishment measures are targeted at the aggressor's vulnerabilities, and threatened as punishment should a given threshold of hostility be crossed.

> …going ‘beyond deterrence’ to respond assertively to hybrid warfare could be crucial to changing the behaviour of hybrid aggressors.

Chapter 5

Responding to hybrid attacks

Beyond deterrence: responding to hybrid attacks

This chapter moves beyond deterrence to focus on taking actions and measures where deterrence has failed.[50] Doing so is necessary to achieve Strategic Goal 3 ('disrupt or prevent an adversary from taking further hybrid aggression') but may also contribute to Strategic Goal 1 and Strategic Goal 2.

Research and analysis during this project has shown that going 'beyond deterrence' to respond assertively to hybrid warfare could be crucial to changing the behaviour of hybrid aggressors.[51] Yet many existing and proposed policies to counter hybrid warfare appear to be biased towards deterrence and resilience.[52] Analysis for this project has identified three possible reasons for this.

- Resilience measures are usually low cost (in terms of the resource and public support required, but also to organize and coordinate) and not generally politically contentious.
- The concept and practice of resilience and deterrence are already widely theorized and relatively well understood.
- More assertive countermeasures can be unpredictable, in terms of the response of the targeted actor, the response of other actors, and unforeseen consequences or second order effects (for example, sanctions).

While hybrid warfare is designed to impede or prevent decisive responses and countermeasures, there are viable ways to respond assertively and move 'beyond deterrence'. This chapter describes the main components to consider in designing a tailored response to hybrid warfare attack.

50 The intent to use these measures can also be communicated as a form of deterrence.

51 See MCDC, (2019), Information Note, *Deterrence by Punishment as a way of Countering Hybrid Threats: Why we need to go 'beyond resilience' in the gray zone*. This information note argues that the limitations of relying on resilience measures to counter hybrid warfare mean that a strategy of deterrence-by-punishment may be more effective.

52 See Annex C for further detail on the current state of countering hybrid warfare policy.

The Countering Hybrid Warfare Response Framework

The Countering Hybrid Warfare Response Framework shown below in Figure 5.1 uses an 'ends-ways-means' model to demonstrate how to determine the basic building blocks of any response to hybrid aggression. This section describes the main components.

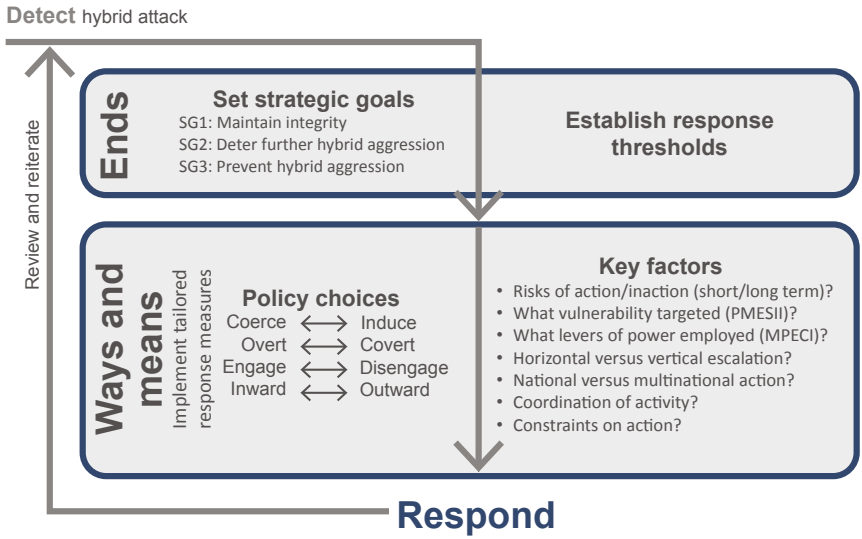


Figure 5.1 – The Countering Hybrid Warfare Response Framework[53]

Ends

The initial dilemma in responding to a hybrid attack is whether to respond at all. Should a response be deemed necessary, the 'ends' (what outcome the response should achieve or contribute to achieving) are set according to the tailored strategic goals and thresholds for action of the responding actor. These should be kept under continuous review to make sure they are appropriate and achievable.

a. Set the strategic goals. If the capacity for independent action (SG1) can be maintained despite an attack – for example where resilience

53 The CHW Response Framework assumes that a hybrid threat or attack has been detected that requires a response (for example, the threat or attack is above a specified threshold for response).

measures already in place could help absorb or withstand attack – then it may be appropriate to take no response. More demanding strategic goals will require more decisive action to deter aggression (SG2) or prevent further attacks (SG3).[54]

b. Establish response thresholds. Governments cannot respond to every incident of hybrid activity. Thresholds for response must therefore be established based on what level of hostility can be reasonably tolerated.[55] Each strategic goal requires a threshold or set of criteria to determine when to respond to achieve each goal. Setting thresholds that take into account why and when to respond to hybrid warfare ensures responses are justified, appropriate and consistent.

Ways and means

Once it has been decided that a response to hybrid aggression is appropriate and the ends have been established, the next step is to identify the specific 'ways' and 'means' that might be employed to achieve the ends. These should be formed by considering policy choices, key factors and levers of power.

Policy choices. Every response to hybrid warfare is shaped first and foremost by the tailored strategic goals of the defending actor to which the response must contribute. The next level of definition can be described by four main 'policy choices'. Taken together they define the character of the response. These elements are interdependent and not mutually exclusive: elements of all of them may feature in some responses.

a. Engage *versus* disengage. This element considers the extent to which the adversary or attack is acknowledged and confronted head-on.[56] A policy that confronts hostile hybrid activity, for example in exposing cyberattacks, can provide effective deterrence. The downside of this approach is that it can legitimize and expose threats that might otherwise be harmless. On the other hand, policy that simply ignores or dismisses an attack as irrelevant or inconsequential can contribute towards preventing its recurrence by denying the adversary the intended effects (such as media coverage). However, the risk of a policy that ignores threats could include a lack of preparedness or public support for subsequent action.

54 See Chapter 2 for more detail on setting strategic goals.

55 See Chapters 2 and 4 for more detail on establishing and communicating response thresholds.

56 This distinction is made for example in Hellman, Maria and Wagnsson, Charlotte, (2017), *How can European states respond to Russian information warfare? An analytical framework*, European Security, Volume 26, Issue 2.

b. Inward *versus* outward. This element considers whether the response is focused inwards towards the defending actors' own population and decision-makers, or outward towards the adversary or the international community. In some cases the response will be entirely inward-focused, for example in educating the population about disinformation. In other cases the focus should be entirely on the adversary, for example, through private diplomatic channels. The impact of one on the other may have unintended consequences, or can be used constructively. For example, inward-focused resilience-building measures may have a deterrent effect on the adversary. Likewise, adversary-focused measures (such as economic sanctions) might reassure the actors' own population that the attacker is being held to account.

c. Overt *versus* covert. Overt action could be classified as public, obvious and official. It can be targeted inward and outward, and can be effective in generating public awareness and support, or exposing adversary action and intent to a wide audience. The downside of overt action includes the unintended consequences of public actions that can be interpreted in different ways by all parties. Covert action can be classified as having a limited audience, being subdued and even deniable.[57] It can be effective in sending direct messages to adversary decision-makers and having direct physical effects that can deter or prevent an adversary from conducting further hybrid attacks (for example, offensive cyberattacks), but can also work against the defender who is potentially ceding control of the public narrative to the aggressor.

d. Coerce *versus* induce. This element considers whether the response is focused on taking assertive measures to coerce the adversary or taking inducement measures to promote cooperation. Coercive measures should seek to exploit the benefits of creative horizontal escalation through credible and creative low-level measures targeted across PMESII vulnerabilities using the MPECI levers of power that impose costs to create coercive effect. On the other hand, attempts at behavioural change are often more successful where inducement can complement coercion (see Infobox 5.1). While the risk of coercion is inadvertent vertical escalation, the risk of inducement is the perception of leniency – which could produce the same result.

57 This distinction (between covert and overt action) was described by Charly Salonius-Pasternak of the Finnish Institute of International Affairs (FIIA) in the first CHW workshop in Helsinki, June 2017.

Infobox 5.1 – Coercive diplomacy and the 'ideal policy'

Countering hybrid warfare can be viewed as a form of coercive diplomacy. Alexander George described coercive diplomacy as a defensive strategy to deal with revisionist actors with three main characteristics: the use of military force is not central (efforts instead rely on diplomacy and other non-military levers); it differs from deterrence because it is a response to an action already taken; and inducements or rewards play an important role.[58]

Peter Viggo Jacobsen's idea of the 'ideal policy' builds upon these foundations to suggest any attempt at coercive diplomacy must include both credible assurances to the adversary against future demands, and an offer of inducement or rewards for compliance.[59] The lessons for countering hybrid warfare (through both deterrence and response) are therefore clear: strike a balance between the 'carrot' and 'stick'.

Key factors. The following key factors are elements to take into account when assessing the policy choices, before selecting and tailoring the measures to be taken in response to hybrid attack.

a. Risk. What are the risks of taking specific action in response to a hybrid attack, and what are the risks of taking no action? One risk of action might be escalation, while one risk of inaction might be further hybrid aggression. All actions have consequences in the short- and longer-term. For example, while the short-term risk of action might be minor escalation, the longer-term risk of inaction might be major escalation by the aggressor.

b. Vulnerability. What PMESII vulnerability will be targeted? For inward resilience measures the vulnerabilities targeted will belong to the responding actor, while for outward responses the vulnerabilities targeted will be those of the aggressor.

c. Lever of power. What MPECI levers of power will be employed? The levers of power used should provide the opportunity to influence the targeted vulnerabilities.

58 Levy, J. S., (2008), *Deterrence and Coercive Diplomacy: The Contributions of Alexander George*, Political Psychology, Volume 29, Number 4.

59 Jakobsen P.V., (1998), Constructing a Theoretical Framework; Chapter 3 in *Western Use of Coercive Diplomacy after the Cold War*, Palgrave Macmillan, London.

d. Horizontal *versus* vertical escalation. A response to a hybrid attack may also exploit the benefits of coordinated horizontal and vertical escalation (see Figure 5.2). While a hybrid aggressor does this to remain under response thresholds and generate complexity, the responder may benefit in the following ways.

- Manage escalation through proportionate responses.
- Manage escalation through asymmetric responses.
- Increase the target 'surface area' through targeting a wider range of vulnerabilities.
- Pursue low-level responses through horizontal escalation that are more credible because they are easier to implement.

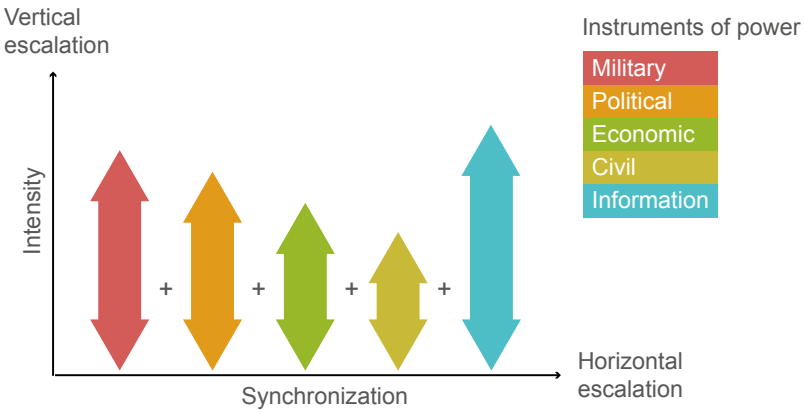


Figure 5.2 – Using the Analytical Framework to consider horizontal and vertical escalation **in response** to hybrid attack

e. National and multinational action. Does the response involve national or multinational activity? A multinational response can provide more varied and effective responses and beneficial second-order effects (such as the perception of solidarity), but can be more difficult to plan, generate and implement.

f. Coordination. As recommended in the CHW1 Analytical Framework, any action to respond to hybrid aggression should be coordinated both across national governments (through dedicated organizational machinery) and between nations (through multinational frameworks).

g. Constraints. The legal basis for responding to hybrid attacks must be clear as one of the defining characteristics of hybrid attacks is the exploitation of legal 'grey areas'. Yet international law allows for an evolving range of responses to a range of aggressive or hostile activity (Infobox 5.2).[60] Responses must also take account of constraints to their implementation which can damage their credibility and impact. For example, the level of public awareness or support for specific measures, the availability of resources (capability and capacity), the nature of the hybrid attack,[61] or attribution of the aggressor.

Infobox 5.2 – International law and hybrid warfare

A distinguishing feature of hybrid warfare is the exploitation of asymmetry. In the legal domain, hybrid aggressors exploit the seams within international law to impede the victim's ability to respond decisively. When combined with coercive measures to specifically deter counteraction, an aggressor can establish a situation of asymmetric advantage. Yet while these tactics might be invidious, there are two key arguments for levelling the playing field from the perspective of international law.

First, states may respond to the use of force in-kind, such as through United Nations (UN) Article 51 and UN Security Council Chapter 7 action. NATO and the European Union both have treaty guarantees to collective action under international law which evolve to meet emerging threats. For example, NATO has declared an intent to respond to cyberattacks and hybrid warfare as an armed attack. International law does not stand still and will be subject to further efforts to increase its 'resilience' to exploitation and subversion.[62]

Second, international law also provides for a wealth of measures to counter hybrid aggression without requiring the use of force. Examples include sanctions, financial protection, capacity building, security sector reform, anti-corruption, resource diversification, education, infrastructure protection, cyber defence, soft power or media regulation. In other words, there is ample legal basis for creative horizontal escalation to counter hybrid warfare.

60 Sari, Aurel, (2019), Hybrid Warfare, Law and the Fulda Gap, in Christopher Ford and Winston Williams (eds), *Complex Battle Spaces*.

61 MCDC, (2018), Information Note, *Fighting Without Firearms: Contending with Insurgents and Soft, Non-Kinetic Measures in Hybrid Warfare*. See Annex A.

62 Sari, Aurel, (2018), *Blurred Lines: Hybrid Threats and the Politics of International Law*, available at https://www.hybridcoe.fi/wp-content/uploads/2018/01/Strategic-Analysis-2018-1-January-Sari.pdf

Responding to hybrid attacks using the MPECI levers of power

This section provides some examples of means to respond to hybrid threats and attacks. Means to deter are covered in Chapter 4. While none of the instruments presented below are new, they are presented together to suggest the benefits of a coordinated approach to responding through horizontal escalation.

a. Military. Military action should be calibrated to ensure proportionality, while maximizing the coercive potential of the military instrument to target the vulnerabilities of hybrid aggressors. The full range of military force options can be used to respond to hybrid attacks, depending on the strategic goals to be achieved. Military force can contribute to resilience measures (SG1), deterrence (SG2) and prevention (SG3).

b. Political. Measures focused on the political domain range from travel restrictions for political officials or incumbents, expulsion of diplomats, suspension of memberships or the withdrawal of voting rights of individual states in international organizations.

c. Economic. The effectiveness of economic measures should not be underestimated – there are many examples of the influence and effect of well-targeted sanctions. Sanctions and financial penalties targeted at individuals (such as freezing assets) can also be effective in the short term. The second-order consequences of sanctions – such as decreased trade and broader impact on societies – may have to be absorbed to create the intended primary effect.

d. Civil. The rule of law is one of the cornerstones of democracy. Public prosecution, like after the presidential elections 2017 in the United States and the public naming of suspects in the Skripal poisonings can be effective. Transparency through public blaming and naming strengthens the trust of the society in public institutions.

e. Information. Measures to support openness and transparency of media through regulation can increase trust and access to information across society. Misinformation and disinformation can be countered through education and exposed through transparency, with legal action available to impose penalties. Offensive cyber measures are quickly becoming more sophisticated.

The approach presented here suggests exploiting horizontal escalation across PMESII sectors using MPECI levers of power to counter hybrid warfare – a kind of modern 'flexible response'. However, further work is required that goes beyond the scope and expertise of this project to fully characterize the contribution and vulnerability across the PMESII/MPECI spectrum. Nonetheless, this handbook offers a framework within which this work can be conducted by policy planners within national and multinational institutions.

Visualizing responses to hybrid attack

Figure 5.3 demonstrates a way of visualizing a strategy to respond to hybrid attack, building on the concepts from CHW1. It shows a mixture of response measures aimed at achieving Strategic Goals 1-3. These measures are mainly targeted at the aggressor's vulnerabilities.

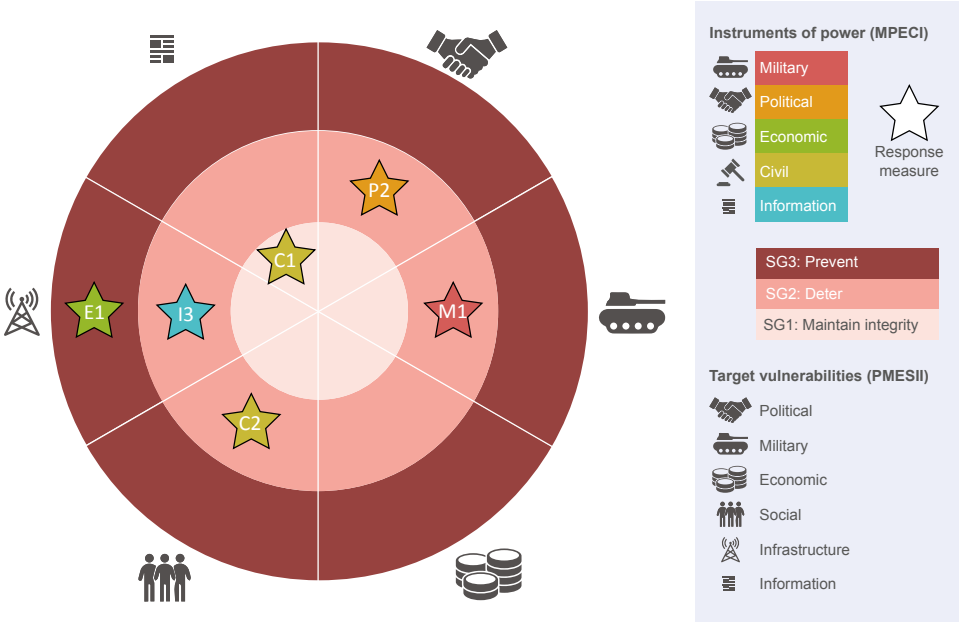


Figure 5.3 – Visualizing responses to hybrid attack

Key points

- If deterrence fails it is necessary to respond to hybrid attack to achieve Strategic Goal 3 (disrupt or prevent an adversary from taking further hybrid aggression). Responses may also contribute to Strategic Goals 1 and 2.
- Going 'beyond deterrence' to respond assertively to hybrid warfare could be crucial to changing the behaviour of hybrid aggressors. Yet many existing and proposed policies to counter hybrid warfare appear to be biased towards deterrence and resilience.
- While hybrid warfare is designed to impede or prevent decisive responses and countermeasures, there are many viable measures with the potential to offer governments options to respond assertively to hybrid attacks.
- Once the aims and response thresholds have been established, a range of MPECI ways and means can coordinated and targeted at the vulnerabilities of the hybrid aggressor to respond through horizontal and vertical escalation.
- Where possible these responses should be combined with inducement and reassurance measures, striking a balance between the 'carrot' and the 'stick.

Notes

> What is clear is that achieving a strategic approach to countering hybrid warfare – including in a crisis – will be easier if the appropriate institutional machinery is already in place.

Chapter 6

Developing institutional machinery

This chapter uses the three components from the CHW Framework to explain the practical aspects of how governments should think about the 'institutional machinery' – the processes, mechanisms, people and skills – required to counter hybrid warfare. It builds upon the key principles set out in CHW1. In particular:

- countering hybrid warfare is a 'whole-of-government' activity;
- countering hybrid warfare requires a multinational approach; and
- rather than creating new institutional machinery, existing institutions, processes and organizations should be adjusted and augmented.[63]

The challenge of achieving such a coherent, coordinated approach across government departments and between nations should not be underestimated. It is difficult to achieve even on issues where an understanding of the problem, a consensus for action and the capacity to act is clear (for example, counterterrorism or climate change). Yet little of these preconditions exist where countering hybrid warfare is concerned. What is clear is that achieving a strategic approach to countering hybrid warfare – including in a crisis – will be easier if the appropriate institutional machinery is already in place.

This chapter therefore offers guidance on how to adjust or augment existing institutional machinery. As with the rest of this handbook, this guidance is intended to prepare the conceptual and intellectual ground for government decision-makers to design and implement policies to counter hybrid warfare.

63 MCDC, (2017), *Understanding Hybrid Warfare*, page 4.

Institutional machinery for detecting hybrid threats

The recommendations for detecting hybrid threats presented in Chapter 3 build upon those made in the original Analytical Framework.[64] The key insight is to differentiate the problem of hybrid warfare situational awareness into monitoring 'known unknowns' and discovering 'unknown unknowns'.

a. Monitoring for known unknowns requires institutional machinery that includes or enables:

- a coordinated approach to the collection, analysis and assessment of data;[65]
- a comprehensive, 'fuzed' picture of threat-assessment data;
- a logical inference of the intent and an accurate picture of the capability of an existing (or potential) hybrid aggressor to reference threat assessments against;
- formalized agreements for information sharing between government departments and within multinational institutions;[66] and
- strengthened working relationships between analysts and decision-makers from across governments and nations.

b. Discovering unknown unknowns requires institutional machinery that includes or enables (as well as the considerations above):

- detecting and reporting anomalies;
- recognizing previously unseen patterns and connections;
- identifying 'weak signals' of developing hybrid threats;

64 MCDC, (2017), *Understanding Hybrid Warfare*, page 4. This recommended a self-assessment of critical functions and vulnerabilities across all (PMESII) sectors and enhancing traditional threat assessment activity to include non-conventional political, economic, civil, international (PECI) tools and capabilities.

65 For example the European Union's 'Hybrid Fusion Cell', NATO's 'Hybrid Analysis Branch' or Finland's 'Security Committee'

66 Such agreements may need to be underpinned by new and amended legislation. For example in Finland legislative amendment was required to support new security committee arrangements. Further detail at https://turvallisuuskomitea.fi/en/security-committee/

- people with the appropriate skills and experience to spot potential threats that have never occurred or been imagined before (such as abductive reasoning, creative thinking and diverse backgrounds); and

- understanding and analyzing (PMESII) vulnerabilities to (MPECI) levers of power to anticipate and prepare for potential attacks.

Both approaches require an analysis and decision-making body that has two key characteristics. First, it must have sufficient breadth of institutional oversight to break down information-sharing 'stovepipes' and cover potential vulnerabilities and attack vectors. Synthesizing this data will facilitate 'pattern discovery' of potential vulnerabilities and modes of hybrid attack. Second, it must have enough institutional authority to gather the wide spectrum of data required, and for its assessments and analysis to carry weight across a variety of stakeholders – some of whom might not traditionally pay attention to threat assessments. For example, the Finnish government's 'Security Committee' has been established in the Prime Minister's office for some of these reasons. It includes analysts dedicated to discovering possible 'unknown unknown' events by collecting and assessing reports of anomalous events across government and society.[67]

Institutional machinery for deterring hybrid aggressors and responding to hybrid attacks

The institutional considerations for deterring hybrid aggressors and responding to hybrid attacks are similar: both require coordinated planning and implementation of measures across the PMESII domains using the MPECI levers of power. The main difference between the two is the implementation of measures targeted towards the hybrid aggressor when responding to hybrid attacks. The following institutional considerations will enable effective deterrence and response through preparing, coordinating and implementing countermeasures.

a. Establish a framework concept across government for countering hybrid threats to which all relevant parties can contribute most effectively. For example, a core element in the Finnish and Norwegian

67 Pasi Eronen, Tiina Ferm, Mika Kalliomaa, Nadja Nevaste, Irina Olkkonen, Juha-Antero Puistola, Finnish Dept of Defense, *The Finnish comprehensive security concept as a model for countering hybrid influencing*, available at https://www.hybridcoe.fi/publication-tags/strategic-analysis/

approach is founded in their respective national 'Total Defence' concepts which describe a whole-of-government approach to a broad range of security challenges and advocates mutual support. Within this framework, various formal and informal forums and civil-military cooperative bodies have been established at central, regional and local level, supporting a common situational awareness.[68]

b. Establish a central decision-making and coordination body with the agility and authority to implement countermeasures in a crisis (for example, in response to a hybrid attack). Ideally this should be collocated with the monitoring and analysis function.

c. Establish domain or sector-specific centres with responsibility for developing and encouraging best practice to counter hybrid threats in their field, thereby increasing overall PMESII resilience. For example, the UK's National Cyber Security Centre advises government and business on vulnerability to cyberattacks.[69]

d. Establishing the policy and practice of contingency planning across governments and between nations for hybrid warfare scenarios and attacks.

e. Develop a countering hybrid warfare 'playbook' through the preparation of measures that can be both threatened as deterrence and implemented as a response. Having this ability (and communicating it) is a deterrent in itself. See Chapters 4 and 5 for more detail on developing measures.

f. Develop a culture of planning and implementing policy across government departments and between nations by default and by design through behaviours, processes, leadership, skills development, relationships and strategic communication.[70] As the saying goes: 'culture eats strategy for breakfast'.

68 See MCDC, (2019), Research paper, *A description of two national conceptual approaches for establishing Hybrid Threat/Hybrid Influence Situational Awareness*, for further detail. See Annex A.

69 Further detail on The National Cyber Security Centre can be found at https://www.ncsc.gov.uk/

70 The UK government's 'Fusion Doctrine' is one example of this approach. For example, 'Building a culture of common purpose across departments requires improved accountability to shift incentives and behaviours towards a more genuinely whole-of-government approach'. For further detail see https://www.gov.uk/government/publications/national-security-capability-review-nscr, page 11. Pasi Eronen, Tiina Ferm, Mika Kalliomaa, Nadja Nevaste, Irina Olkkonen, Juha-Antero Puistola, Finnish Dept of Defense, *The Finnish comprehensive security concept as a model for countering hybrid influencing,* available at https://www.hybridcoe.fi/publication-tags/strategic-analysis/

g. Regular education, training and exercise of the personnel and institutional machinery involved in countering hybrid warfare is necessary to establish clear communication, understand roles and responsibilities, practice effective cooperation, coordinate plans and procedures, and develop mutual knowledge about needs and capacities.

In addition, the following points should be considered regarding resilience – the main component of deterrence by denial. Chapter 4 covers this in greater detail.

a. Establishing a body with an overview of resilience or preparedness across government and society.

b. Strengthening links to the private sector and civil society to build awareness of both the threat and what they can do about it. For example, to guard against damage to privately owned infrastructure and services, to educate civil society about disinformation, or encourage business resilience.[71] These links and relationships also contribute to more comprehensive hybrid warfare situational awareness (see above).

c. Developing a culture among civil society and the private sector that supports threat awareness and resilience, that benefits from both 'top-down' (government-led) and 'bottom-up' (society-led) efforts to enhance resilience and preparedness by whoever is best placed to take action.

Countering hybrid warfare: implications for defence

Countering hybrid warfare is a whole-of-government activity that relies predominantly on non-military tools. Yet the role of defence remains an important one because of the unique contributions it can make to detecting hybrid threats, deterring hybrid aggressors and responding to hybrid attacks.[72]

The unique capabilities of defence forces contribute to deterring aggressors from both conducting hybrid warfare in its own right, and to resorting to conventional armed aggression. With this in mind, any significant adjustment

71 See Helsinki Region Chamber of Commerce, (2018), *Business Community and Hybrid Threats*, available at http://view.24mags.com/mobilev/bbc43250c51aa3c0b599cb18066f3c2b#/page=1

72 Many of the insights in this section also apply in principle to other departments of state or instruments of power. Based on MCDC, (2019), Information Note, *Countering Hybrid Threats: Establishing Conceptual Clarity in UK Defence.* See Annex A.

to the composition of national defence forces that reduces their contribution to traditional deterrence (for example, through the ability to conduct high-end war fighting) requires a careful and clear-eyed assessment of what constitutes the most likely and the most dangerous threats to the nation.

To support policies to counter hybrid warfare, national defence forces must be able contribute to national and international efforts to detect hybrid warfare, deter hybrid aggressors and respond to hybrid attacks. Taken together, these requirements will have three broad implications for defence.

a. Coordination. The need for improved coordination between the use of force and the other levers of power across government and between nations to make sure the defence contribution to a whole-of-government approach to countering hybrid warfare is appropriate and effective, supported by routine contingency planning for hybrid threats.[73]

b. Options. Substantive revisions to the way defence forces are organized, resourced and equipped to offer governments more options below the threshold of armed conflict to deter and respond to hybrid aggression.[74]

c. Resilience. A renewed approach to both defence's contribution to national or 'homeland' resilience, and the resilience of defence itself to hybrid warfare.[75]

73 For example in UK Fusion Doctrine, or under renewed 'total defence' efforts in Sweden, Finland, Austria and other nations. MCDC, (2019), Research paper, *The Finnish comprehensive security concept as a model for countering hybrid influencing.* See Annex A.

74 This insight is central to the new US *Joint Concept for Integrated Campaigning* (JCIC). The JCIC describes how 'the Joint Force plays an essential role in securing and achieving national aims in conditions sometimes regarded as outside the military sphere: competition below the threshold of armed conflict', page iii, available at http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257

75 See MCDC, (2019), Information Note, *A review of UK Defence's contribution to homeland resilience and security in light of the changing global context.* In discussion during the CHW project, this idea of revitalizing homeland resilience was referred to as '21st Century total defence' – in reference to the Cold War concept of 'total defence' that was central to many nations' strategies for national defence and resilience.

Key points

- Countering hybrid warfare requires appropriate governmental 'institutional machinery': the processes, mechanisms, people and skills to implement strategy.
- Countering hybrid warfare is a 'whole-of-government' activity, requires a multinational approach and should exploit and augment existing institutions, processes and organizations where possible.
- For detecting hybrid warfare, both 'monitoring' and 'discovery' require an analysis and decision-making body that has broad institutional oversight and authority.
- Both deterring and responding to hybrid warfare requires coordinated planning and implementation of measures across the PMESII domains using the MPECI levers of power.
- Although countering hybrid warfare is a whole-of-government activity that relies predominantly on non-military tools, the role of defence remains an important one because of the unique contributions it can make to detection, deterrence and response.

Annex A

Research papers, information notes and case studies

Information notes[76]

- *Understanding Hybrid Warfare*, (2017), Erik Reichborn and Patrick Cullen.
- *Hybrid War and its Countermeasures*, (2018), Dr Robert Johnson (University of Oxford Changing Character of War Centre, Pembroke College).
- *Fighting Without Firearms: Contending with Insurgents and Soft, Non-Kinetic Measures in Hybrid Warfare*, (2018), Professor Michael L. Gross (The University of Haifa, Israel).
- *Can hybrid attacks be deterred? And if so, how do we do it?*, (2018), a report prepared for the UK Development, Concepts and Doctrine Centre (DCDC).
- *Deterrence by Punishment as a way of Countering Hybrid Threats: Why we need to go 'beyond resilience' in the gray zone*, (2019), Heine Sørensen and Dorthe Bach Nyemann (Institute for Strategy, Royal Danish Defence College).
- *'A Deadlier Peril': The Role of Corruption in Hybrid Warfare*, (2019), Lt Col Dave Allen (UK Defence Academy).
- *The State of Current Counter-Hybrid Warfare Policy*, (2019), Albin Aronsson (UK DCDC).
- *A review of UK Defence's contribution to homeland resilience and security in light of the changing global context*, (2019), Dr Tim Benbow, Dr Tim Bird and Dr Rod Thornton Defence Studies Department (King's College London) for UK DCDC.
- *Hybrid Warfare: Understanding Deterrence*, (2019), a report prepared for UK DCDC.

76 Available at https://www.gov.uk/government/publications/countering-hybrid-warfare-information-notes

- *Countering Hybrid Threats: Establishing Conceptual Clarity in UK Defence*, (2019), by Sean Monaghan (UK DCDC).

Research papers[77]

- *Hybrid War and Its Countermeasures: A Critique of the Literature*, by Dr Robert Johnson (University of Oxford Changing Character of War Centre, Pembroke College), available at https://www.tandfonline.com/doi/abs/10.1080/09592318.2018.1404770

- *A description of two national conceptual approaches for establishing Hybrid Threat/ Hybrid Influence Situational Awareness*, Tiina Ferm, Pasi Eronen, Nadja Nevaste, Irina Olkkonen, Juha-Antero Puistola (Finnish Dept of Defense); and Narve Toverød, Alf Christian Hennum, Stein Malerud, Håvard Fridheim (Norwegian FFI). Available on request from the authors.

- *Gray Zone Concept: Competition Short of Armed Conflict*, Col Bonifacio Gutiérrez de León (Spanish Directorate for Doctrine and Research).

- *Countering Hybrid Warfare Policy Framework: Methodology and Overview of Findings* and *CHW Policy Framework Data* (MS Excel), Albin Aronsson (UK DCDC)

- *(How) is Russian Doctrine Talking About Hybrid Warfare?*, a report prepared for UK DCDC.

- *Strategic Goals of Counter-Hybrid Strategies*, Reto Ulrich Flühmann, Dr Daniel Fuhrer, and Gian-Luca Stössel (Swiss Armed Forces Staff).

- *Detecting Hybrid Warfare*, Dr Patrick Cullen and Dr Njord Wegge (NUPI).

- *What does 'best practice' for resilience against hybrid threats look like? and What means are available to deter hybrid threats?*, Lukas Bittner (Austrian Federal Ministry of Defence).

- *Hybrid Warfare and Deterrence*, Emily Robinson (Canadian Department of National Defence, DRDC).

77 Not published as MCDC information notes, these are available online or by contacting the authors.

Case studies[78]

- *Austria's 'Comprehensive National Defence'*, Lukas Bittner (Austrian Federal Ministry of Defence).
- *Perejil Island: The Spanish Response to the July 2002 crisis with Morocco*, Javier Jordan (Department of Political Science, University of Granada).
- *Countering Hybrid Warfare Case Studies*,[79] Dr Robert Johnson (University of Oxford Changing Character of War Centre, Pembroke College).
- *North Korean Cyber Operations and Lessons from Ukraine*, Neil Chuka and Emily Robinson (Canadian Department of National Defence, DRDC).
- *Case Study and Conditioning Factors of the Fight Against Hybrid Enemies: The Battle for Mosul*, by Col Gabriel Martínez Valera (Spanish Directorate for Doctrine and Research).
- *How did the British Government and Security Forces deploy in Northern Ireland to deter the Provisional Irish Republican Army from pursuing its prolonged insurgent/terrorism campaign?*, Peter Hanley (UK DCDC).
- *Case Study: Annexing Of Crimea*, LTC Cezary Pawlak and CDR Jarosław Keplin (Polish Armed Forces).
- *Case Study Deterrence Israel-Hezbullah*, Reto Ulrich Flühmann, Dr Daniel Fuhrer, and Gian-Luca Stössel (Swiss Armed Forces Staff).
- *Hybrid Warfare in Salisbury: analysing the West's Response*, Kim van Winkel (UK DCDC).
- *Monitoring and visualizing hybrid activity – a UK food-for-thought paper for the MCDC Countering Hybrid Warfare project*, a report by UK Dstl prepared for DCDC.

78 Available on request from authors.
79 Four case studies: Kashmir; South China Sea; Kargil Offensive; and Counter-Daesh.

Annex B

Visualizing countering hybrid warfare: examples

This section contains three generic examples of a strategy to counter hybrid warfare, visualized using the countering hybrid warfare tools introduced in this handbook. Each example is characterized using the following information.

a. The title characterizes the essence of the strategy.

b. The strategic goals the strategy is aiming to achieve, ranging across:

- SG1: maintain capacity for independent action;
- SG2: dissuade or deter an adversary from hybrid aggression; and
- SG3: disrupt or prevent an adversary from taking further hybrid aggression.

c. A broad description of the thresholds of hostility at which counteraction will be taken. These thresholds may differ across different domains, but should be considered as whole due to the synergistic nature of hybrid warfare. Thresholds may or may not be communicated to the aggressor (see Chapter 3 and 5 for detail).

d. The measures employed to deter – whether by denial, focused on the defender's PMESII vulnerabilities, or by punishment, focused on the aggressor's PMESII vulnerabilities – or respond to hybrid warfare.

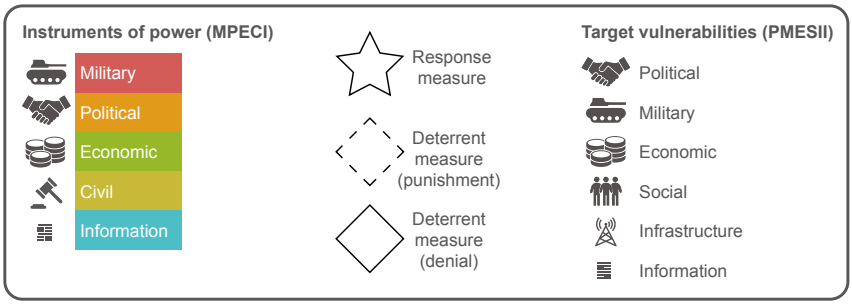


Figure B.1 – Key to visualizing hybrid warfare examples

Example 1 – ‘resilient’

Strategic goals

Mostly maintaining capacity for action (SG1).

Thresholds

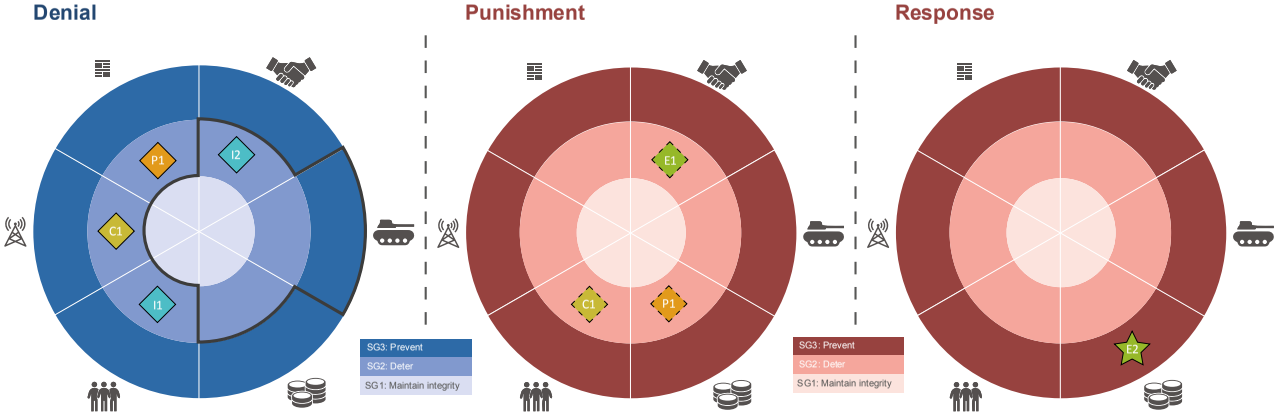
Most concerned about social, infrastructure and information domains.

Measures

Deterrence by denial
P1: publicly attribute and seek international action against foreign interference
C1: introduce critical infrastructure protection legislation and extra funding
I1: population-focused communications campaign warning and educating against disinformation and interference

Deterrence by punishment
E1: prepare multinational economic sanctions targeted at key industry sectors in response to political interference

Response
E2: implement multinational economic sanctions targeted at key industry sectors



Example 2 – ‘measured’

Strategic goals

Maintaining capacity for action (SG1) and deter hybrid threats (SG2).

Thresholds

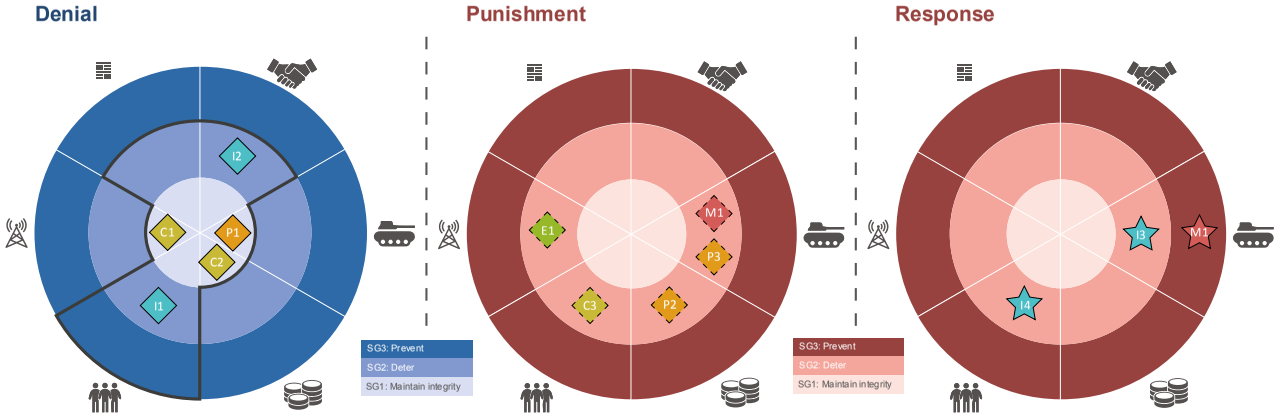
Most concerned about military, economic and infrastructure domains.

Measures

Deterrence by denial
C1: introduce critical infrastructure protection legislation
C2: enhance financial transparency and anti-money laundering legislation
P1: political statements and agreements against commons violations (airspace and territorial waters)

Deterrence by punishment
M1: increased freedom of navigation operations manoeuvres (air and sea)
E1: prepare multinational economic sanctions targeted at key infrastructure provision
P3: action in multinational political forum targeted at aggressive use of the military

Response
I3: public attribution of illegal and aggressive military manoeuvres
M1: enhanced rules of engagement to enable more assertive response to territorial violations
I4: information campaign to expose aggressive posture and malpractice in aggressor state towards their population



Example 3 – ‘assertive’

Strategic goals

All strategic goals.

Thresholds

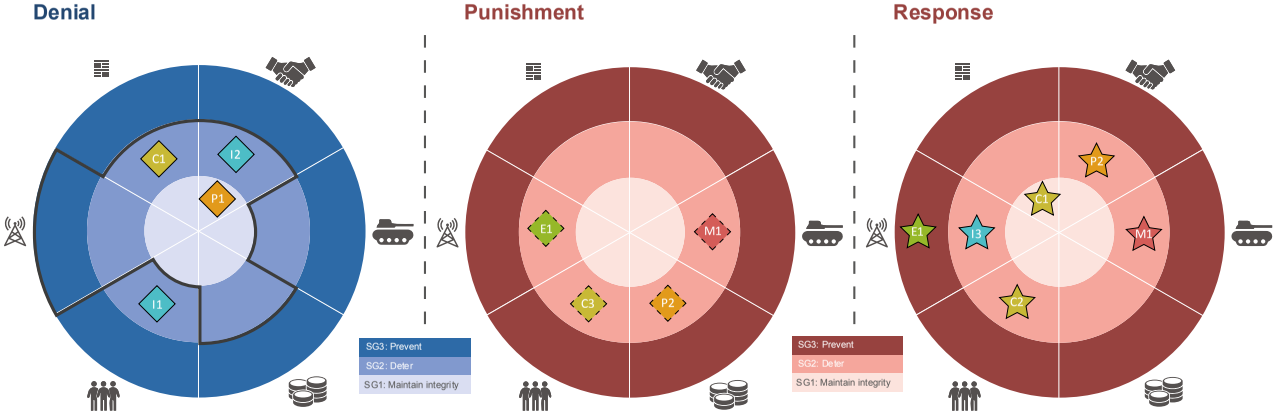
Most worried about effects in the military and social domains; not worried about infrastructure.

Measures

Deterrence by denial
C1: strengthening media regulation
I2: increasing transparency of political decisions

Deterrence by punishment
M1: conduct freedom of navigation operations at sea
E1: sanction the provision of infrastructure services from third parties

Response
M1: conduct freedom of navigation operations at sea
E1: sanction the provision of infrastructure services from third parties
I3: expose threats to critical national infrastructure



Annex C

The current state of countering hybrid warfare policy

As part of the countering hybrid warfare project the current state of countering hybrid warfare policy was analyzed. The purpose was to identify trends in existing or proposed policy measures to inform the development of better policy. A framework was established to analyze and compare policies from a range of sources. While not intended to be exhaustive or widely representative, this analysis provided 'food for thought' within the scope of the countering hybrid warfare project. A full analysis of the findings of this research is available as an information note.[80] Table C.1 below gives an overview of the range of sources and number of policies analyzed.

Type of publication	Number of publications	Total number of policies
Think tank papers	8	68
European Union and NATO official texts	4	21
MCDC CHW case studies	6	21
Total	**18**	**110**

Table C.1 – Summary of publication type and number of policy measures

The framework used for analysis examined three main components:[81] whether the policy in question was 'defensive' or 'offensive' in nature;[82] the instrument of

80 MCDC, (2019), Information Note, *Countering Hybrid Warfare Policy Framework: Methodology and Overview of Findings* and *CHW Policy Framework Data* (MS Excel).

81 The policy analysis framework was devised by Pasi Eronen, Iiris Saarelainen and Simon Källman. Most of the data entry and analysis was performed by Albin Aronsson.

82 This was judged from the perspective of the hybrid aggressor in question. In terms of the CHW Framework, 'defensive' options generally relate to 'deterring' hybrid aggressors (mainly through deterrence by denial, for example, through resilience measures) while 'offensive' options generally relate to 'responding' to hybrid attacks (but also cover deterrence by punishment, where the offensive measure can be threatened as punishment).

power used (MPECI);[83] and the type of vulnerability targeted (PMESII).[84]

Key findings

Offence-defence balance. The large majority of measures proposed were defensive in nature. These measures are focused on resilience, capability and capacity building, and increasing the defender's ability (across government and society) to withstand, absorb and recover from hybrid attacks. Several factors may explain this trend and are explored in Information Note, *The State of Current Counter-Hybrid Warfare Policy*. In summary, while the ideal balance between defensive and offensive remains unclear, there are more offensive measures available to defending actors than it may seem. Furthermore, righting this imbalance may be the only way to change the behaviour of hybrid aggressors.[85]

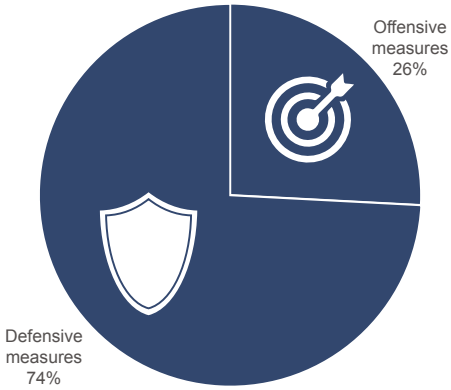


Figure C.1 – Offence-defence balance of hybrid warfare countermeasures

Defensive measures: targeted vulnerability. The majority of defensive measures were targeted at building resilience in the political and informational spheres of society, supported by increased intelligence-gathering measures. This makes sense insofar as hybrid warfare often targets political decision-making, which is often informed and supported – especially in democratic societies – by freely

83 In the original analysis the acronym 'DIMEFIL' (defence, information, military, economic, finance, intelligence and legal) was used instead of 'MPECI'. In this annex the results are presented using MPECI by equating diplomacy to political, finance to economic, and intelligence/legal to civil.

84 For defensive measures the vulnerability targeted belongs to the defending actor; for offensive measures the vulnerability targeted belongs to the hybrid aggressor.

85 See the case made for going 'beyond resilience' in MCDC, (2019), Information Note, *Deterrence by Punishment as a way of Countering Hybrid Threats: Why we need to go 'beyond resilience' in the gray zone*.

available public information. Yet these are also the most difficult components of the liberal-democratic societal model to protect. Paradoxically, overdoing resilience and government-led intervention here may undermine the very fabric of society that is trying to be preserved in the first place.

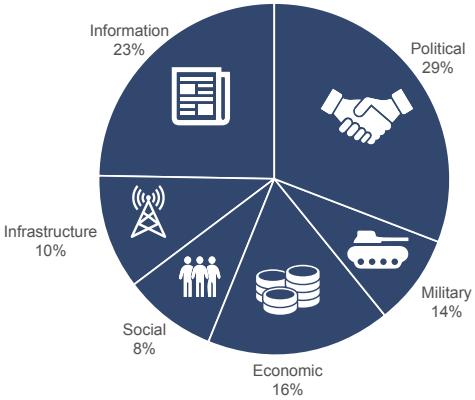


Figure C.2 – Defensive measures – targeted vulnerability

Offensive measures: instruments of power used. The reliance on the military instrument in response to hybrid threats and attacks shown here seems to highlight a shortfall in the ability of Western governments (the majority of the sources analyzed) to summon creative ways to escalate horizontally through offensive options. Over-reliance on such a 'blunt' instrument may lead either to inaction until it is too late, or the potential for provocation and miscalculation by being heavy-handed. Instead, alternative offensive means should be found to diversify the 'playbook' for countering hybrid warfare.

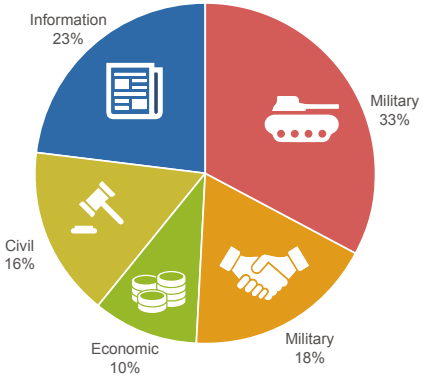


Figure C.3 – Offensive measures – instruments of power used

Offensive measures: targeted vulnerability. Measures targeted at political vulnerabilities to counter hybrid warfare are the 'foundation' of any offensive response to hybrid attack. The political nature of states who exploit hybrid warfare often contain elements antithetical to the liberal-democratic model such as centralized power, corrupt elites, control of information flows or lack of transparency, making obvious targets for measures such as anti-corruption and political support to third-party (for example, non-European Union) states. However, the very nature of such regimes makes them pre-hardened to such measures. Once again, this survey reveals the lack of other options beyond politics for horizontal escalation and punitive measures to threaten and cause damage to the interests of hybrid aggressors. Without these options being developed and deployed, the behaviour of hybrid aggressors is unlikely to change. The analysis suggests these options are available – for example, through exploiting 'issue linkage' and going on the media offensive.

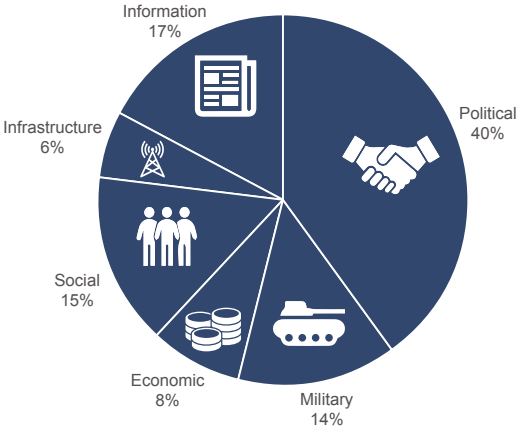


Figure C.4 – Offensive measures – targeted vulnerability

Annex D

Table top exercise and matrix game: key findings

The final workshop of the CHW2 project included a fictional scenario-based table top exercise (TTX) and matrix game to help test and refine the CHW Framework.

The scenario used was a fictional one based on nations, events and geography created for the game. The scripted scenario described the escalating hybrid threat from a series of events that affected critical functions across society, set within the political context of an approaching election. The same scenario was used for the TTX and matrix game.

Both games focused on the opportunities, constraints and possible challenges in seeking to employ the principles described in the CHW Framework. They put players in the position of national decision-makers with the job of formulating policy and implementing actions to counter the apparent use of hybrid warfare.

a. The TTX guided the players through a facilitated, structured discussion based on the unfolding scenario. It did not force players to make decisions, but enabled them to reflect on the situation to identify

concerns, constraints, risks and opportunities, while considering how the CHW Framework might be applied in practice.

b. The matrix game focused on applying the CHW Framework in practice when exposed to allied and adversarial actors in real time.[86] It allowed further exploration of the principles identified in the TTX, exposing players to feedback from intelligent and reactive opponents and helping them understand the consequences of decisions taken earlier in the game.

Lessons and limitations

A small selection of lessons and limitations from the game are provided below to demonstrate the kind of insight generated.

- 'Red' (aggressor) was able to exploit 'Blue' (defender) vulnerabilities such as diverse threat perceptions and ineffective coordination between Blue nations and Blue government departments.
- In the game the various governments broadly had equal capacity and resources, whereas in the real world this would not be the case.
- Some players were interested in attribution while others would self-attribute and use it for their own political objectives.

86 Matrix gaming is a free-form gaming method in which a structured process of discussion among players is employed to resolve game actions and generate a narrative. Matrix games help turn concepts into actions and explore them in a dynamic and emerging problem space.

- Open Red hostile actions – albeit below thresholds of decisive response – meant there was often little need to detect activity or seek attribution.

- There was little opportunity to test methods and approaches to detecting hybrid warfare, but 'deter' and 'respond' were tested throughout the game.

- There was often little incentive for Red to be 'deterred' by Blue actions. It was also difficult for Blue to determine whether Red had been deterred or not – this was often due to a lack of understanding about Red's thresholds (or 'red lines').

- There was not enough involvement of non-state actors. For example, private sector companies are often victims of state-sponsored cyberattacks.

- It was very difficult to simulate long-term economic effects in game such as high public spending, sanctions and brain-drain.

- Red´s failures often forced them to escalate their activities.

- Misunderstandings and misperceptions often lead to the more radical and escalatory activities.

- Asymmetries between the *status quo* and revisionist actors in risk appetite, red lines, strategic culture, ethics and norms often played out.

- In the real world dealing with a long-term strategy requires a long-term counter-strategy. It was difficult to allow for this in the game.

- More time was required to develop policy and strategy during the game before the negotiation and action phases started.

List of CHW project contributors

Name	Nationality	Organization	Email
Dorthe Bach Nyemann	Denmark	Royal Danish Defence College	Dony@fak.dk
Lukas Bittner	Austria	Defence Policy Division, Ministry of Defence	lukas.bittner@bmlv.gv.at
Pasi Eronen	Finland	-	-
Major Mike Fenton	Canada	Canadian Armed Forces	Mike.Fenton@forces.gc.ca
Colonel Reto Ulrich Flühmann	Switzerland	Swiss Armed Forces Joint Operations Command	reto.fluehmann@vtg.admin.ch
Dr. Daniel Fuhrer	Switzerland	Armed Forces Development, Swiss Armed Forces Staff	daniel.fuhrer@vtg.admin.ch
Col Bonifacio Gutiérrez	Spain	Directorate of Research, Doctrine, Organization and Materiel (DIDOM), Spanish Army	bonifacio@et.mde.es
Lt Col (GS) Christian Heiser	Austria	Military Strategic Division, Ministry of Defence	christian.heiser@bmlv.gv.at
Javier Jordan	Spain	Department of Political Science, University of Granada	jjordan@ugr.es
CDR Jaroslaw Keplin	Poland	Doctrine and Training Centre, Polish Armed Forces	j.keplin@ron.mil.pl
Col Markus Kohlweg	Austria	-	markus.kohlweg.8@bmlvs.gv.at
Irina Lönnqvist	Finland	-	irina.lonnqvist@mpk.fi
Col Gabriel Martínez-Valera	Spain	Joint Center for Concept Development (CCDC), Ministry of Defense	gmvalerag@hotmail.com
Nadja Nevaste	Finland	Prime Minister's Office,	nadja.nevaste@vnk.fi
Cdr Juha-Antero Puistola	Finland	Defence Command Finland	juha-antero.puistola@mil.fi
Mr. Charles C. Pattillo Jr.	United States	Multinational Operations Division (MOD), U.S. Department of Defense	charles.c.pattillo2.civ@mail.mil

Name	Nationality	Organization	Email
Lt Col Cezary Pawlak	Poland	Doctrine and Training Centre of the Polish Armed Forces	cezarypawlak@o2.pl
Emily Robinson	Canada	Defence Research and Development Canada, Centre for Operational Research and Analysis (DRDC CORA), Department of National Defence	Emily.Robinson@forces.gc.ca
Dr Hanna Smith	Finland	Director of Research and Strategic Planning, European Countering Hybrid Threats Centre of Excellence	hanna.smith@hybridcoe.fi
Heine Sørensen	Denmark	Senior Lecturer, Institute for Strategy, Royal Danish Defence College	hes@fmn.dk
Com (sg) Narve Toverød	Norway	Norwegian Defence Research Establishment (FFI)	nto@ffi.no
Scarlett Waitzmanová	Czech Rebublic	Defence Policy and Strategy Division, CZ Ministry of Defence,	waitzmanovas@army.cz
Axel Weisshaupt	Germany	Land Operations Doctrine Department, German Army Headquarters	axelweisshaupt@bundeswehr.org

Glossary

Centre of gravity analysis is a military-planning methodology derived from Carl von Clausewitz's book *On War* to identify the 'source' or 'hub' of power in a system.

Critical functions are activities or operations distributed across the political, military, economic, social, information, infrastructure (PMESII) spectrum; the discontinuance of which would lead to the disruption of services that a working system (for example, a state, its society, or a subsection thereof) depends on. Critical functions can be broken down into a combination of actors (for example, individuals or organizations), infrastructures (for example, 'critical' national power grids) and processes (for example, legal/jurisdictional, technical, political).

Deterrence by denial aims to undermine the ability of the adversary to achieve their objective in the first instance through, for example, 'hardening' the target.

Deterrence by punishment aims to persuade the adversary the costs of achieving their objective will be prohibitive by threatening retaliation to aggressive action.

Effects are a change of state of an entity as the result of actions against specific vulnerabilities of a target system.

Horizontal escalation is the applied combination of multiple military, political, economic, civil, informational (MPECI) means.

Hybrid warfare is the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects.[87]

Hybrid warfare self-assessment is a continuous national process to identify critical functions and find vulnerabilities within the PMESII spectrum.

Institutional machinery are the processes, mechanisms, people and skills required in national governments and multinational institutions to implement strategies to counter hybrid warfare.

87 MCDC, (2017), *Understanding Hybrid Warfare*.

Instruments of power are elements of the MPECI environment. When these elements are 'weaponized' the instruments of power can become tools of attack.

Non-linearity refers to unanticipated effects of hybrid warfare attacks that are not causally linear. They are the result of synergistic interactions of hybrid warfare attacks in which the whole is greater than the sum of their parts. Non-linear effects cannot always be predicted by the attacker or defender.

Resilience is the ability of society and government to absorb, withstand and recover from disruption and external shocks. Measures to increase resilience contribute to deterrence by denial.

Strategic goals are the aims of the strategy to counter hybrid warfare. Strategic goals reflect the level of ambition of the defending actor.

Synchronization of means is the ability of a hybrid warfare actor to effectively coordinate the instruments of power (MPECI) to achieve the desired effects in both horizontal and vertical ways.

Synchronized attack packages (SAPs) are specific MPECI means that are synchronized and tailored to specific vulnerabilities that are used in a hybrid warfare attack.

Threshold is determining the magnitude or the intensity of a functional status (for example, the 'stress level') of one's critical functions to be exceeded to achieve a specific status (for example, normal or crisis). It is the the level of hostility at which counteraction will be taken.

Vertical escalation is the intensified use of one specific means.

Vulnerabilities are personnel, activities, resources or processes within a potential target that are susceptible of being exploited or created by a potential adversary.

For more information, contact: MCDCsecretariat@apan.org