MCDC

Multinational Capability Development Campaign

MCDC Countering Hybrid
Warfare Project:

Countering Hybrid Warfare 3 Guidance for planners

A Multinational Capability Development Campaign project

Distribution statement

This document was developed and written by the contributing nations and organizations of the Multinational Capability Development Campaign (MCDC) program community of interest. It does not necessarily reflect the views or opinions of any single nation or organization, but is intended as a recommendation for national/international organizational consideration. Reproduction of this document and unlimited distribution of copies is authorized for personal and non-commercial use only. The use of this work for commercial purposes is prohibited; its translation into other languages and adaptation/modification requires prior written permission.

Executive Summary

Countering Hybrid Warfare 3 (CHW3) builds on the advice provided in CHW1, *Understanding Hybrid Warfare* and CHW2, *Countering Hybrid Warfare* to try and provide practical advice and guidance for planners to better understand hybrid warfare and what can be done to anticipate and mitigate its effects. It is aimed at those new to the subject and aims to accelerate their understanding of it to make them more productive. For more established planners, the document seeks to broaden their understanding while not being definitive or prescriptive. The document is not designed to provide a definitive understanding of the problem, this would be too difficult. It is intended to build upon key areas that may be of interest to planners in the hope that it will engender debate, thinking and discovery of evolutionary solutions to an evolutionary problem. It is not intended to replace planning guidance; it is designed to supplement them.

Chapter 1 provides a short overview of the previous two documents in this series, which will provide sufficient information to allow the reader to understand the points being made later in this publication. The reader is strongly recommended to read both CHW1 and CHW2 for a thorough understanding of them.

Chapter 2 focuses on how adversaries may use the military, political, economic, civilian and informational (MPECI) instruments of power to influence or impact our ability to conduct operations and how they may seek to do this through a gradual approach. It seeks to broaden considerations beyond those traditionally thought about by military planners to enable them to have a more holistic understanding of how an adversary may seek to impact our ability to operate.

Chapter 3 looks at what planners may do to mitigate the impact on their plans of adversarial actions. It examines familiar ground but does so through a hybrid warfare lens that highlights where marginal changes may be beneficial to any planning organisation and their plans. It provides considerations that are grouped into three main areas: understanding, preparation and operating.

Chapter 4 is a handrail guide to operational design and considerations to be borne in mind at every step of the planning process. This is for planners to build upon with their own knowledge and experience and provide an aide memoire for hybrid warfare.

Chapter 5 looks to future trends that may influence planning.

Contents

Introduction

What is the Multinational Capability Development Campaign Countering Hybrid Warfare project?

1. The Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare[1] (CHW) project aims to help national and multinational security and defence personnel understand, anticipate and counter the effects of hybrid warfare. The term hybrid warfare has been adopted with the following description: the synchronised use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effect.[2]

2. The first phase of this project, CHW1, produced a theoretical model and understanding of what hybrid warfare is. The second phase of the project, CHW2, produced a handbook designed to inform national and multinational security and defence policy for countering hybrid warfare based on three elements: detect, deter and respond. This handbook, CHW3, builds on the first two to form three complementary handbooks.

Purpose

3. The purpose of this handbook is to educate strategic- and operational-level military planners about the potential impact of hybrid warfare on their plans and what they might want to consider when conducting advance or crisis response planning in a hybrid warfare environment. While the information in this handbook can act as entry level education for those new to the subject of hybrid warfare, it is also designed to act as a handrail for more experienced planners. It is not designed as a substitute for previous CHW work, and all are encouraged to read CHW1 and CHW2.[3]

Application

4. While the hybrid warfare environment is not new or unique, it is necessary that military commanders and staff adapt how they operate. This handbook accepts that the fundamentals of most military planning processes at the strategic and operational levels remain valid, at present. As such, this guidance is not intended to replace existing planning tools and processes, but rather to supplement them by explaining how they can be adapted to better account for the potential impact of hybrid warfare. Consequently, this guidance is designed to be used for all categories and stages of planning and for any

[1] MCDC has adopted the term hybrid warfare to include hybrid threats.
[2] MCDC, *Understanding Hybrid Warfare,* 2017, page 3.
[3] These publications are available at https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare

operation. Furthermore, this guide accepts as a starting point that countering hybrid warfare is a 'whole-of-government' activity that requires a comprehensive approach in which the military may be a supporting actor to other instruments of power. Therefore, the points made in this handbook may be applicable to other government departments. It is not designed to be a definitive document, rather it is a start point intended to help the planner understand and adapt to the fluid hybrid warfare environment by prompting them to consider more factors than they would normally have done.

5. The handbook is organized into five chapters.

- Chapter 1 recaps the understanding of hybrid warfare from CHW1 and CHW2 and provides the necessary information to allow the reader to understand the fundamentals of the hybrid challenge.
- Chapter 2 helps the reader to better understand how an adversary might use hybrid warfare to impact strategic and operational planning
- Chapter 3 guides the planner on how to modify existing or implement new practices that could help mitigate these actions.
- Chapter 4 takes the planner through the generic planning steps, providing advice and guidance at each stage on what to consider.
- Chapter 5 offers recommendations for longer-term institutional, organizational and cultural changes that may help with success in hybrid warfare.

‘In Strategy the longest way around is often the shortest way there. A direct approach to the object exhausts the attacker and hardens the resistance by compression, whereas an indirect approach loosens the defender’s hold by upsetting his balance.’

Liddell Hart

Chapter 1 – Understanding the hybrid warfare challenge

1.1. Much has been made of hybrid warfare and its impact over the past few years. This in turn has created confusion and doubt in the minds of many who want to try and understand it so that they can anticipate and prepare for its impacts. What is different about hybrid warfare today is the increasingly connected world, and the increasing speed of that connectivity, which brings many strengths and vulnerabilities that an adversary can potentially exploit.

1.2. The Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare (CHW) project sought to bring clarity to the topic of hybrid warfare. The first phase of the project, CHW1, published two key documents that were released to the MCDC community on 31 October 2016: a CHW Baseline Assessment and a CHW Analytical Framework.[4]

1.3. The Baseline Assessment completed two tasks. First, it provided a critical review of hybrid warfare literature (to date) and created a common set of 'MCDC CHW terminology' with which to start analysing hybrid warfare. Second, it identified gaps in the understanding of hybrid warfare and drew out common characteristics of both non-state and state hybrid warfare that could then be used to develop the generic analytical components for the second deliverable – the CHW Analytical Framework. A truncated version of the Baseline Assessment was made public under the title 'What is Hybrid Warfare?'

1.4. The CHW Analytical Framework completed three tasks. First, it provided a pragmatic and policy-oriented heuristic model for understanding hybrid warfare composed of three interlocking parts: the defender's critical functions and vulnerabilities; the attacker's synchronized use of multiple instruments of power with horizontal and vertical escalation of them; and the linear and non-linear effects of an attack. Second, it provided a series of graphic visualizations of a hybrid warfare attack and how to detect them, including real time monitoring of one's critical vulnerabilities via the use of baselines, thresholds and indicators. Third, it outlined a series of policy recommendations for countering hybrid warfare that included: 1) conducting national self-assessments of vulnerabilities to hybrid warfare; 2) enhancing national threat assessments to include the coordinated and ambiguous use of non-military tools; and 3) the creation of a whole-of-government process (at the national and multinational levels) to understand, detect and respond to hybrid warfare. A modified version of the original Analytical Framework was made publicly available under the title *Understanding Hybrid Warfare*. CHW1 also produced an annex document of five case studies used to test the application of the CHW Analytical Framework.

[4] MCDC, *Understanding Hybrid Warfare,* 2017, page 7.

1.5. Building on the research and ideas in CHW1, CHW2 produced a handbook titled *Countering Hybrid Warfare*. This provided detailed theoretical guidance for a CHW strategy based on three elements: detection, deterrence and response.

1.6. **Detect.** The CHW1 Analytical Framework described why hybrid threats may be difficult to detect and how a traditional adversary-centric threat analysis is inadequate for doing so.[5] The CHW2 project proposed differentiating warning intelligence for potential hybrid attacks into two separate categories: 'known unknowns', identified by monitoring the environment for indicators; and 'unknown unknowns', identified by discovery or the process of capturing and then correctly interpreting information related to potentially hostile adversarial actions not previously conceived.[6] 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; these are the unknown unknowns. A useful way of developing this concept for hybrid warfare warning intelligence is to differentiate monitoring from discovery.[7]

1.7. **Deter.** ‘Hybrid deterrence’[8] 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. Therefore, effective ‘hybrid deterrence’ requires updating traditional approaches to deter modern hybrid threats. To do so, the CHW2 project examined the basic principles of deterrence,[9] how they are challenged by hybrid warfare and how to address these challenges by establishing a ‘hybrid deterrence’.

1.8. **Respond.** The CHW2 project examined the challenge of responding to hybrid threats or attacks and created a framework for making decisions about doing so.[10] 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’.[11] 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. Furthermore, when assessing the policy choices and before the selection and tailoring of response measures to hybrid attacks,

[5] MCDC, *Understanding Hybrid Warfare*, 2017, page 10.
[6] MCDC, *Countering Hybrid Warfare,* 2019, page 26.
[7] MCDC, *Countering Hybrid Warfare*, 2019, page 22.
[8] Deterrence of hybrid actors as opposed to ‘conventional deterrence’ of conventional warfare actors.
[9] MCDC, *Countering Hybrid Warfare*, 2019, page 40.
[10] Ibid., page 52.
[11] Engage versus disengage, inward versus outward, overt versus covert, and coerce versus induce.

certain factors need to be considered.[12] The counter-hybrid strategy developed in CHW2 is represented in Figure 1.

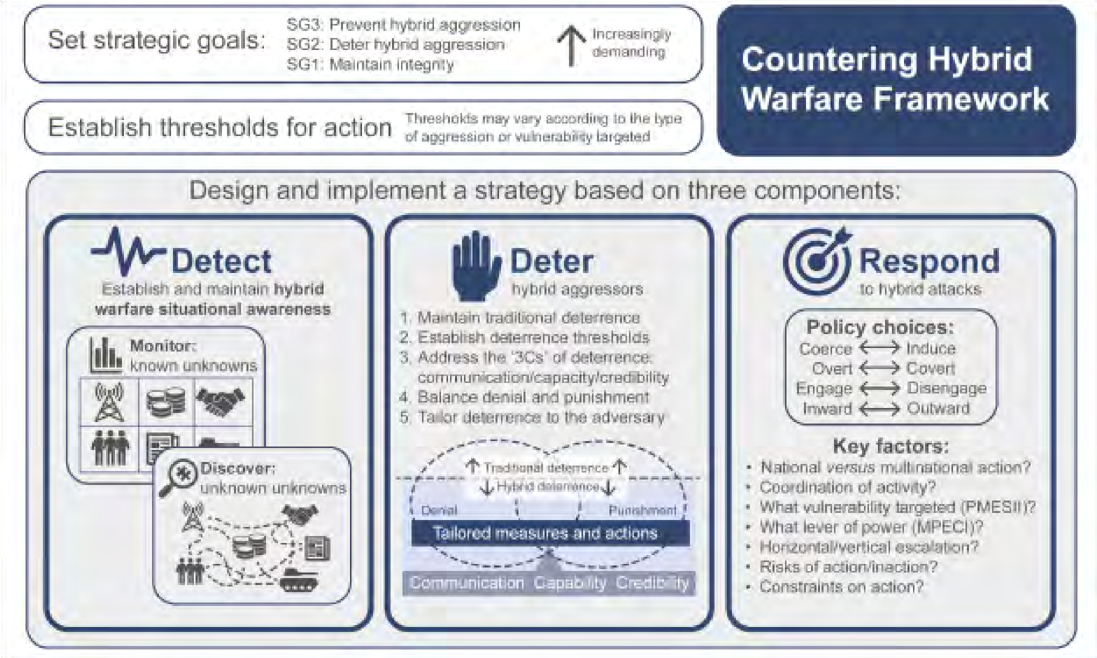

Set strategic goals:
SG3: Prevent hybrid aggression
SG2: Deter hybrid aggression
SG1: Maintain integrity
Increasingly demanding
Establish thresholds for action
Thresholds may vary according to the type of aggression or vulnerability targeted
Countering Hybrid Warfare Framework
Design and implement a strategy based on three components:
Detect
Establish and maintain hybrid warfare situational awareness
Monitor: known unknowns
Discover: unknown unknowns
Deter
hybrid aggressors
1. Maintain traditional deterrence
2. Establish deterrence thresholds
3. Address the '3Cs' of deterrence: communication/capacity/credibility
4. Balance denial and punishment
5. Tailor deterrence to the adversary
Traditional deterrence
Hybrid deterrence
Denial
Punishment
Tailored measures and actions
Communication
Capability
Credibility
Respond
to hybrid attacks
Policy choices:
Coerce ⟷ Induce
Overt ⟷ Covert
Engage ⟷ Disengage
Inward ⟷ Outward
Key factors:
• National versus multinational action?
• Coordination of activity?
• What vulnerability targeted (PMESII)?
• What lever of power (MPECI)?
• Horizontal/vertical escalation?
• Risks of action/inaction?
• Constraints on action?

Figure 1 – Detect, deter and respond to hybrid warfare

So what for planning?

1.9. Eisenhower's maxim that 'plans are useless, but planning is everything' is true in a hybrid warfare environment. Since hybrid warfare impacts the ability to plan at all levels, a deliberate intent to counter the effects of hybrid warfare must be at the heart of all policy and strategy.

[12] For example, risk of specific actions, which vulnerability should be targeted, which instruments of power should be used, which kind of escalation is most suitable, is a national or multinational action a better approach, what (legal) constraints are in place and who will coordinate the response.

Chapter 2 – The impact on plans

2.1. Chapter 2 aims to help planners prepare by explaining how hybrid warfare may impact plans. It outlines what an adversary may be seeking to achieve and then looks at how they might achieve those aims. It is advice and guidance to help the planner form their own solutions by building on this advice, it is not a definitive check list.

How an adversary may employ hybrid warfare

2.2. The liberal international order is clearly changing and is increasingly under pressure[13] and hybrid warfare is very much connected to this. Globalization, migration, geopolitical shifts, the changing nature and balance of power, increased digitalization and connectivity, and increasing ease of access to technological and social resources have raised vulnerabilities within states and societies to new levels and are changing the security paradigm. This has resulted in a complex and ambiguous situation with severe challenges for international institutions and states. Hybrid warfare uses the current transformation processes by exploiting vulnerabilities to change the international order to their own favour.[14]

2.3. Hybrid warfare adversaries pursue their interests by taking advantage of ambiguity[15] and gradual shifts ('death by a thousand cuts'[16]) in rights and norms, perverting the principle of 'rule of law' to one of 'rule by law'.[17] That means that hybrid warfare can mask an adversary's true objectives, which can hinder any response. Hybrid warfare adversaries influence where they have an advantage and may exploit vulnerabilities across the whole political, military, economic, social, informational and infrastructure (PMESII) spectrum.

2.4. Even if most of the influence occurs outside of the traditional military domains, crises can still escalate to a stage where a military response is inevitable. Thus, if a state or alliance chooses to respond with armed forces, they need to assume that an adversary will undertake different hybrid warfare approaches to delay, hinder and disrupt the preparation, activation and deployment of military forces.

[13] Mearsheimer, J., 'Bound to Fail – The Rise and Fall of the Liberal International Order', *International Security*, Volume 43, Number 4, Spring 2019, pages 7–50. https://doi.org/10.1162/ISEC_a_00342

[14] Bolt, P., 'Sino-Russian Relations in a Changing World Order', *Strategic Studies Quarterly*, Volume 8, Number 4, Winter 2014, pages 47–69.

[15] Ambiguity is defined here as hostile actions that are difficult for a state to identify, attribute or publicly define as coercive uses of force. Ambiguity is used to complicate or undermine the decision-making processes of the opponent. It is tailored to make any type of response difficult. In military terms, it is designed to fall below the threshold of war and to delegitimize or render irrational the ability to respond with the use of military force. Source: MCDC, *Understanding Hybrid Warfare*, 2017, page 10.

[16] MCDC, *Understanding Hybrid Warfare*, 2017, page 15.

[17] Ginsburg, T. and Moustafa T., *Rule by Law: The Politics of Courts in Authoritarian Regimes*, Cambridge, UK: Cambridge University Press, 2008. https://summit.sfu.ca/item/15130.

2.5. Hybrid warfare is sometimes termed sub-threshold[18] with the threshold being defined as the line between peace and war. There are, in fact, several thresholds that elicit different responses with no clear line between them. Hybrid warfare exploits these thresholds between different stages of a decision-action cycle, see Figure 2, to disrupt the ability to make effective decisions and implement associated actions.[19]

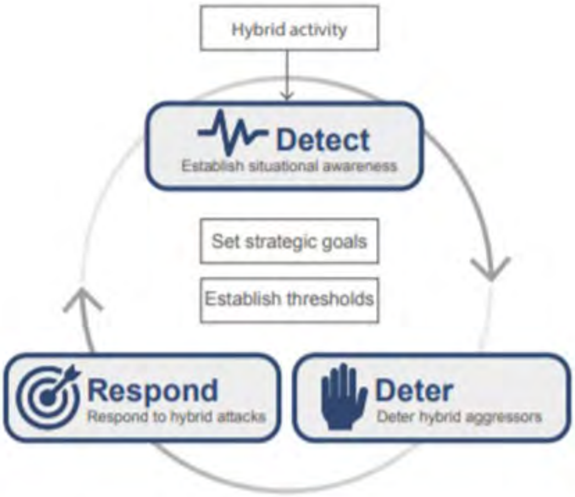


Figure 2 – The Countering Hybrid Warfare decision-action cycle

2.6. In a hybrid warfare scenario, a decision-action cycle is impeded where ambiguity exists over the elements of hybrid warfare being employed. As such, the thresholds themselves become unclear. An adversary may want to keep its activities below the threshold of detection; if detected, below the threshold of understanding; if understood, below the threshold of decision; and if decided, below the threshold of response. To set the conditions to achieve their aims, adversaries will attempt to make the level and strength of every threshold ambiguous by disrupting the ability of other actors to gather information, make sense of it, decide what to do – collectively or not – and then act. ‘Offensive success’ in hybrid warfare is achieving an aim without an adversary responding effectively. ‘Defensive success’ is taking the right actions that cause an adversary to desist from their offensive actions and return to normal competition. Therefore, an adversary will take great effort to focus on complicating and impeding the decision-action cycle.

2.7. The aims and objectives of an adversary engaged in hybrid warfare are, usually, deliberately obscured and may range from seeking some form of revision in the international system, that they consider to be to their advantage, to preventing anything

[18] 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). Source: MCDC, *Understanding Hybrid Warfare*, 2017, page 32.
[19] Termed OODA loop after the stages of observe-orientate-decide-act which then links back to observe the impact of your action.

they may view as disadvantageous to them. Where previously adversaries may have sought to achieve their aims through force of arms, in the contemporary operating environment the thought of war may be too costly in all but existential scenarios due to the anticipated disruption that would likely be caused to the economic and international systems on which they depend.

2.8. Adversaries may therefore try and achieve their aims by gradually changing international rules, institutions, the balance of power or the distribution of international trade. If an actor is not dependent on being part of the international system then they may resort to violence more readily. This change, known as measured revisionism, is where an adversary seeks changes to the rules-based international order (RBIO) that was established to provide stability and leadership to the global community. Measured revisionists do not want to cause mayhem since they are engaged in the international system. But, they cannot achieve their aims from operating inside the rules and norms of the existing system and therefore they seek alternative paths outside of it, some legitimate,[20] some not. Whether or not a state is a revisionist state is a matter of perspective. What is important to understand is why they are a revisionist state.

2.9. Gradualism is an approach adopted by those revisionist actors that have the benefit of time to achieve their aims. They can take an incremental approach in their hybrid warfare strategies which, in general, are not designed to achieve a rapid and decisive response but rather to slowly unfold, gradually pushing boundaries in ways that do not merit a robust military response. When designed to negate the efficacy of deterrence, gradualism is especially effective against coalitions, where opinions on the level and type of response can be divided. Gradualism can be broadly divided into two approaches, both of which can be one-off events or cumulative, depending on the response to them.

> a. **Salami slicing.**[21] Due to the serious nature of war, few countries are likely to go to war for a minor infringement by another. This lack of a robust response provides further encouragement to the actor to adopt ever more incremental approaches towards achieving their intended goal and so it slowly builds until the adversary achieves their aims and any response is too little too late. Incremental approaches may erode deterrence and reassurance provided by third party

[20] In 2016, China established the Asian Infrastructure Investment Bank in direct competition to the World Bank to allow them to control the pace of development in Asia.

[21] Professor Branislav Slantchev, *Introduction to International Relations Lecture 8: Deterrence and Compellence*, University of California, 2005, page 4. http://slantchev.ucsd.edu/courses/ps12/08-deterrence-and-compellence.pdf

countries.[22] This approach has pitfalls such as provoking a sudden violent response, which was not wanted.

b. **Fait accompli.**[23] A fait accompli is where a nation rapidly commits an act that surprises others and leaves them with no choice but to accept the outcome, unless they are prepared to fight. Unlike salami slicing they are decisive acts. But, like salami slicing, they are generally small or justifiable enough in scale to allow an adversary to get away with them. This approach, like salami slicing, leaves the defender with little choice but to accept it.

2.10. In seeking to achieve their aims, an adversary will almost certainly employ a variety of methods that will ideally be unobtrusive, deniable, ambiguous and involve deception. This is because they will not want to attract the attention of other nations or organizations that might stop them from achieving their aims and objectives. Once objectives have been achieved, any period of uncertainty is over and they are established and feel secure enough to openly resist any physical confrontation, or certainly make it too costly to dislodge them, they may then become more belligerent. One of the key risks is accidental escalation through misunderstanding and miscalculation.

2.11. The challenge in all of this is to understand how the adversary may achieve their aims, whether they are strategic, operational or tactical, what tactics they will employ to achieve them and how their intentions may emerge. It is important to remember that no two adversaries are the same; they do not think the same, act the same, view the world in the same way or seek the same objectives; there is no ‘one-plan fits all’ solution. Each adversary must be approached as an individual problem, unique from other adversaries and previous events and, consequently, any response or plan must be tailor-made.

2.12. Hybrid warfare adversaries may seek to achieve their aims using the military, political, economic, civilian, informational (MPECI) instruments of power, exploiting new or emerging technologies to help. In general, non-military instruments of power are preferred when employing hybrid warfare because they make a military response harder to justify.[24] An adversary will increase or decrease pressure in one or all of the MPECI instruments of power, see Figure 3, in a coordinated manner necessary to achieve their aims while trying to stay below any response threshold.

[22] In 1939, both Britain and France failed to check the gradualist advance of Germany. This emboldened Germany, which was surprised when the Allies declared war after the invasion of Poland.

[23] Altman D., ‘By Fait Accompli, Not Coercion: How States Wrest Territory from Their Adversaries’, *International Studies Quarterly*, Volume 61, Issue 4, December 2017, pages 881–891. https://doi.org/10.1093/isq/sqx049

[24] Multiple instruments are used generally it is weakness in one of the MPECI meaning states resort to others. Military superiority for us will force an adversary to use alternatives. In: Ucko, D., ‘Nobody puts IW in an Annex: it’s time to embrace irregular warfare as a strategic priority’, *Modern War Institute*, 2020. https://mwi.usma.edu/nobody-puts-iw-in-an-annex-its-time-to-embrace-irregular-warfare-as-a-strategic-priority/

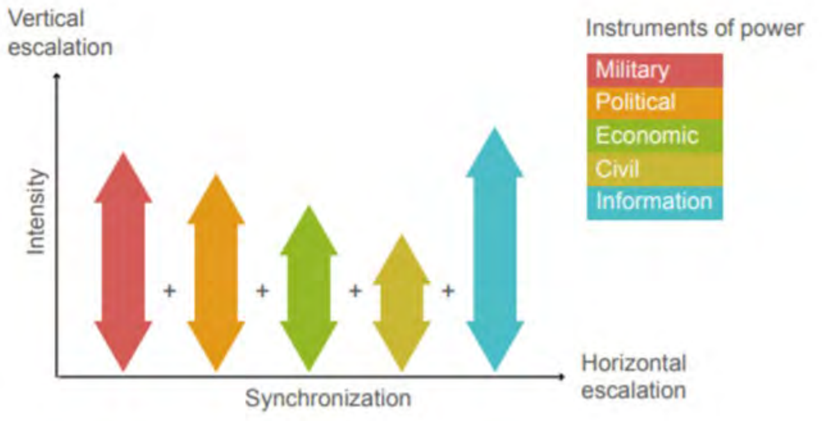


Figure 3 – The MPECI instruments of power

2.13. The military instrument available to an adversary will probably be well known and understood. However, militaries are expensive and need to be justified to political masters; the so-called Gerasimov doctrine arose from this very point.[25] As such, in the early stages of a campaign, adversaries may seek to use their militaries in low-key support of non-military aims. Due to their aggressive posture, military resources may be used carefully and for conducting activity that remains below the threshold of armed conflict as the risk of miscalculation and accidental escalation may be assessed as too high. However, once an adversary is well-established in achieving their aims, it should be expected that the conventional military will be used overtly, as by then the risk of miscalculation and escalation may be viewed as having reduced sufficiently and a victim state may consider the time for a military response has passed. The covert and then overt involvement of the military in support of an adversary's aims and objectives needs to be anticipated.

2.14. Military proxies present an alternative to direct military force. The use of proxies has taken on a renewed vigour as their actions are deniable. Proxies can take many different forms in hybrid warfare, can be difficult to control and may present as many vulnerabilities to their sponsors as they do opportunities in achieving their aims.

The Soviets, via the Stasi, raised and supported proxy organisations in the West during the Cold War. The Baader-Meinhof gang conducted attacks against North Atlantic Treaty Organization (NATO) forces including an attack on the Supreme Allied Commander Europe (SACEUR) in 1979. In 1985, Iran used Hezbollah to kidnap and murder the Central Intelligence Agency's (CIA's) Head of Station in Beirut.

[25] Galeotti, M., 'I'm sorry for creating the Gerasimov doctrine', *Foreign Policy*, 2018. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

2.15. One of the key aims of an adversary will be the creation of political uncertainty in their chosen target to create distractions that prevent a government or alliance from focusing on the real aims of the hybrid warfare event unfolding in front of them, thus delaying or preventing a timely and effective response. This may come in many different forms but will be based on where an adversary sees the greatest gain whilst remaining below any threshold.

2.16. Economic instruments are powerful tools that adversaries will use to their full advantage to help them achieve their aims. Careful consideration needs to be given to the global economic situation and what potential or real adversaries are doing and what this means. Subtle changes in control of ports or other local agreements could have a significant impact on a plan. An adversary will have made their own estimate on where they see critical dependencies for others and will be targeting them.

2.17. In democracies, the link between a society and its elected leaders is pivotal to effective responses. The increasing frequency of low-threshold, ambiguous or deniable attacks, such as cyber, disinformation or influence operations, may erode the link between the people and government of the target nation making political leaders reluctant to respond as their populations may not support them in any action. Deniability will be a key consideration, as attributing an attack to an adversary may galvanise the will of the people they seek to undermine. Attacks on civilian aspects of everyday life may impact the ability of the military to respond due to distractions caused by any disruption.[26]

2.18. Criminality offers an adversary a highly useful way to attack or undermine the civilian aspects of their target as criminals exist everywhere and their activities, on behalf of a client, can be deniable. Criminal proxies could be used to intimidate opponents, push boundaries, compromise friendly militaries and attack people opposed to their objectives. Criminality and its role in hybrid warfare must be fully understood.

2.19. Corruption is an intrinsic part of everyday life in certain parts of the world, in others it is the exception. There are two principle forms, psychological and physical, and the effects of which appear in four guises. The first is an enabler, allowing other events to happen, facilitating access, causing delay or enabling compromising materiel to be obtained. Second, it can amplify existing grievances. Third, it can cause mass disruption by undermining the faith in governments to do their job properly, creating fertile ground for exploitation. Finally, it can cause a distraction from the real issues. In some countries, key individuals will be more than just corrupt, they will also have strong links to criminality. These links present additional challenges to any ability to respond to adversaries as any actions will, rightly, be bound by standards of behaviour, morals and ethics that adversaries will not be.

[26] Van Haaster, J. and Roorda, M., ‘The impact of hybrid warfare on traditional operational rationale’, *Militaire Spectator*, Volume 185, Number 4, 2016, pages 175–185.

2.20. Adversaries will want an in-depth understanding of their target's vulnerabilities across all domains and dimensions. They will have thought through second and third order dependencies, identified where vulnerabilities exist and may seek to disrupt or exploit them. Corruption and criminality may be used to cause a slow-down in unloading of supplies, cause delays in onward movement or higher the price of contracts for the delivery of services; it can even impact training and safety standards.[27] To create these effects, adversaries may mobilize agitators or ordinary civilians to commit a lawful act, such as striking, protesting outside a base or blockading a bridge or exit from a port.

2.21. Information will form a central part of any overt hybrid warfare event with the adoption of several narratives that will develop over time. An adversary will likely have conducted target audience analysis and be prepared to use all possible mediums to ensure that it spread its message as widely as possible. The ambiguous nature of hybrid warfare means that these narratives may cause confusion or sow doubt and division whilst attempting to sustain the adversary's legitimacy and credibility. This is done by creating a lack of confidence in any counter-narrative, especially in liberal democracies where free speech is a fundamental human right. An adversary's narrative will seek to undermine the link between the people and their government. Both the post-Soviet military thinkers, Dugin and Panarin emphasised in their work that informational uncertainty leads to political uncertainty.

[27] LaGrone, Sam, USNI News, 'Paying the Price: The Hidden Cost of the 'Fat Leonard' Investigation', 24 January 2019. https://news.usni.org/2019/01/24/paying-price-hidden-cost-fat-leonard-investigation The impact on the Pacific Fleet was not only the loss of resources but also the culture of mistrust from the ensuing investigation and curtailment of training due to restrictions.

We do not see things as they are.

We see things as we are.

Anaïs Nin

Chapter 3 – Mitigating hybrid warfare

Introduction

3.1. The tenets[28] and characteristics[29] of hybrid warfare, together with the effects created by hybrid warfare actors,[30] create significant challenges how to understand, prepare for and operate against a hybrid warfare adversary. Chapter 3 provides considerations for how to better prepare for and mitigate the impacts of hybrid warfare on plans and operations. The points raised here are a start point to initiate thinking and discussion and not a definitive solution. To be effective the reader must develop their understanding on the subject.

Part 1 – Understanding considerations

Breadth and depth

3.2. In order to counter hybrid warfare and its effects it is important to have as broad an understanding as possible, particularly of areas that are not ones of traditional military focus. This will provide a deeper appreciation of what an adversary may target, why and how. To achieve this depth of knowledge, it will be necessary to broaden any stakeholder community beyond the whole of government into business, industry, non-governmental organizations, academia and further afield. This will ensure the best possible chance of identifying vulnerabilities and dependencies that are key to military outputs as well as the most effective solutions, which may not be military ones.

3.3. This depth of understanding is built up over years of analysis and observation, rather than pulled together at short notice. As the necessary breadth and depth of understanding required may have to come from civilian experts,[31] it will be necessary to cultivate a pool of security cleared individuals who are used to working in the team. If there is a lack of understanding, then it must be sourced.

[28] Gradualism, ambiguity, deniability and deception.

[29] The combined use of multiple instruments of power to achieve asymmetric effects through targeting and expanded range of vulnerabilities; a synchronized attack package that exploit both horizontal and vertical axes of escalation; an emphasis on creativity and ambiguity to achieve synergetic effects (including in the cognitive domain).

[30] These are based on the following three interdependent elements: (1) critical functions and vulnerabilities; (2) synchronization of means; and (3) effects and non-linearity.

[31] These could be from anywhere within or out with government, the more diverse your information the better.

3.4. When developing understanding, the key differentiator between standing defence or crisis response plans is time. More time to prepare means a greater depth and breadth of understanding can be achieved. Plans can be more thoroughly prepared, rehearsed and red teamed, but that increases the chances of the plans being anticipated and responses to them developed by an adversary. Less time means that there is a reduced chance of the plan being revealed, but limited opportunities for a highly original plan. Maintaining a firm baseline understanding is critical to reducing such risk in times of rapid response.

3.5. As individuals, organizations and cultures we all see the world and its problems through our own lens, bringing with us our assumptions, biases and preconceptions. Every individual and society has their own blueprint of right and wrong and it is when people impose their values and worldviews onto others that conflict starts. Avoiding conflict starts with understanding – not only our own goals but understanding other perspectives.[32] When seeking to understand it is important to approach from two perspectives, etic and emic. Etic is viewing a culture or society from your own perspective. This can be revealing but can also lead to a skewed perspective of adversaries and their motives, leading to potentially misleading conclusions. Conversely, the Emic perspective, the ability to view a situation from the point of view of an adversary, may reveal insights that might otherwise have been dismissed. Motives, especially, need to be examined from both an Etic and Emic perspective. These views are worth exploring as you capture their political, military, economic, social, information, infrastructure, physical environment and time (PMESII-PT) factors to understand an adversary's strengths, vulnerabilities and their escalatory dynamics, how they might escalate and how they might view their adversary's escalatory options. Understanding an adversary's escalatory dynamics may prevent a misunderstanding and inadvertently lead to crossing a threshold.

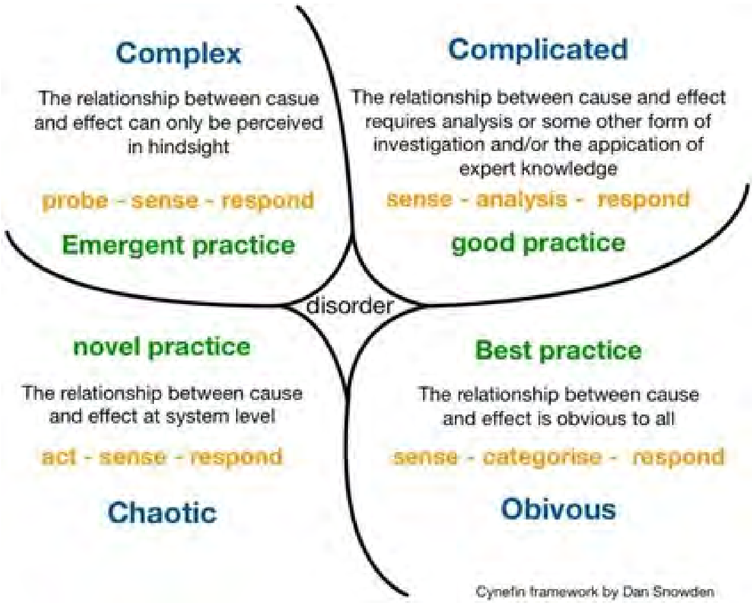
Understanding the operating environment.

3.6. The operating environment is best understood as a complex adaptive system. Complex adaptive systems are characterized by detail and behavioural compexity[33] where it is impossible to control events or understand all relationships. Whilst an actor may control a stimulus event, they cannot be certain what the outcome or responses will be as there are too many variables that can impact the chain of events. Therefore, once an act has been initiated it is the team that can respond most quickly with a response to that input, ideally in a way that is not anticipated by the adversary, that will most likely seize the initiative and force their adversary onto the defensive.

[32] For more information see: https://www.emicconsulting.co.uk/

[33] Lundqvist, S., 'Why teaching comprehensive operations planning requires transformational learning'; *Defence Studies*, 15:2, pages 175–201.

3.7. Understanding is more important than ever in a complex adaptive system, although by its very nature it should be accepted that it will never be fully understood. There is a risk that, in order to understand it, a complex environment may be over simplified and viewed as a complicated one. This will overlook some of the interrelated factors that can lead to increased chances of being surprised or increased ambuguity, which leads to decision inertia. There are many tools to help increased understanding of a complex system such as alternative thinking and variety calculus,[34] but these will not provide total understanding. It is impoprtant to remember that within a complex system, there will also be simple and complicated problems as well as chaos; these are best represented by the Cynefin model, as illustrated in Figure 4. Due to the vast number of complex interactions, understanding is best achieved by persistent analysis that is refreshed and challenged repeatedly.


Complex
The relationship between casue and effect can only be perceived in hindsight
probe - sense - respond
Emergent practice
Complicated
The relationship between cause and effect requires analysis or some other form of investigation and/or the appication of expert knowledge
sense - analysis - respond
good practice
disorder
novel practice
The relationship between cause and effect at system level
act - sense - respond
Chaotic
Best practice
The relationship between cause and effect is obvious to all
sense - categorise - respond
Obivous

Cynefin framework by Dan Snowden

Figure 4 – Cynefin model: making sense of problems

3.8. Developing and maintaining a global and regional outlook across the military, political, economic, civilian and information (MPECI) instruments of power, will start to give an understanding of where an adversary may seek effect. Maintaining a global perspective is important, as different instruments may be used in other parts of the world to threaten the success of a plan in another part. Continuous monitoring may make it possible to see threats emerging in the geopolitical landscape. Membership of collective bodies brings many strengths for detection, analysis and response but they may also bring vulnerabilities, particularly if a collective decision is required for any response. A thorough

[34] For more information see: Rosie, J.F. and Cooper Chapman, C., *Understanding complex environments (Edition 2.0) A Reference Guide for Commanders.*

analysis should identify such vulnerabilities, even if they sit outside the military lever, and the impact of a hybrid warfare attack on plans.

3.9. Understanding a friendly nation's PMESII-PT/areas, structures, capabilities, organizations, people and events (ASCOPE) is a useful starting point in developing understanding of friendly strengths and vulnerabilities and should also be viewed from an adversary's perspective. Look for vulnerabilities that can be exploited by hybrid warfare to cause friction or shape public opinion, but be prepared for 'zero day' vulnerabilities.[35] It is unlikely that any one area will provide the full understanding so combining all aspects will be necessary. Specific considerations by area are as follows.

a. Understanding the government's current strategy on countering hybrid warfare, including such things as thresholds for specific areas, escalation or de-escalation, attribution or non-attribution, constraints or freedoms? What is the national deterrence policy and how does the military contribute? What objectives are being proposed, are they ambiguous or unclear? Is there transparency in the funding of political parties? Is corruption part of everyday life? Which government departments have control of the other instruments of power? Does the political climate create vulnerabilities, such as letting contracts for critical national infrastructure to foreign companies that are obligated to their national governments?

b. In any cross-government response to hybrid warfare, is the military supporting or supported by other government departments? What has the military been asked to do or is it required to develop response options? Which contractors provide key support, and does that present vulnerabilities such as the ability to project and sustain the force or regenerate equipment? What are you reliant on for success? Which nations and allies are important and may need support in any response to an attack? Where are the potential geographic points of tension?

c. How strong is the economy? What areas are vulnerable to strategic shocks? Private companies often control significant aspects of public life (for example, supermarket chains for food supply) so what arrangements are there for communicating with them or sharing information? What are the economies of allies like, are they vulnerable?

d. Are there sources of grievance such as economic inequality, religious freedoms, racial inequality and immigration, real, perceived or historical? Where are there influential or significant ethnic diasporas living? Are there any malign

[35] 'Zero day' vulnerabilities are those that cannot be resolved. It is important to recognize that there will always be vulnerabilities, what is important is the ability to respond to fix a vulnerability once it is identified. See https://pure.uva.nl/ws/files/17279930/Militaire_Spectator_4_2016_Roorda_Van_Haaster.pdf

actors or criminality within the population who are prepared to use violence and act outside of the law for their own ends or others? Are there benign actors who can influence societal groups to support or oppose operations?

e. Where does the population get their information from? What is the level of trust in government information? Are there vulnerabilities in the information environment such as limited press freedoms, state ownership of media outlets or access to foreign sources?

f. Is access to critical national infrastructure information required? Who is responsible for cyber and physical security? How could an adversary deny critical infrastructure that might be needed for enabling operations?

g. How does the physical terrain influence plans? Does climate change affect the plan? What impact might it have on natural resources? Are there any areas of national dispute that could be exploited by an adversary? How does the physical terrain influence political thinking?

h. The role of time is very important. Are there any national anniversaries, upcoming elections or societally significant days that may be contentious? Do seasonality and the weather have the potential to affect events, for example, public demonstrations are more likely in good weather, is there a dependence on an adversary for resources such as energy supplies, and does this provide a lever for an adversary to use?

The information environment

3.10. The information environment is a model used for understanding how audiences interpret events that happen in the world around them. This means understanding which audiences are relevant to the hybrid warfare scenario, what their perceptions of events are, and what channels and means can be used to influence them. Initial audience segmentation should identify those audiences which are friendly, neutral or hostile. Segmenting audiences allows planners to identify where effects – both desired and undesired – might take place. Understanding the information environment is important.

Data sources and analysis.

3.11. Data is central to understanding hybrid warfare and its use is important to success. A wide range of data sources are required from across government and private sources. By combining data sets, so called ‘big data’ can be created. Big data was originally the scale of data needing to be processed, now it is increasingly associated with the use of predictive analytics, user behaviour analytics or other advanced data analytics methods that reveal new insights with a military application. Key to this is artificial intelligence and machine learning, which can be used to process big data and augment or replace human decision-making in its analysis. 'Thick data' is data brought to light using qualitative, ethnographic research methods that uncover people's emotions, stories and models of their world. Both big and thick data need to be combined to develop a depth of understanding.

The electromagnetic environment.

3.12. The electromagnetic spectrum is not only a transversal function for all the physical and non-physical domains in which military operations currently occur, it is also a fundamental element for the maintenance and development of life, both occupational and leisure. Most of the critical infrastructure and systems that support and facilitate life are based on the proper use and management of the electromagnetic spectrum. This has meant that in recent conflicts, especially those that have occurred in cities or other built-up areas, the effective management of the electromagnetic spectrum has been paramount.[36]

3.13. The electromagnetic spectrum is particularly important in hybrid warfare as it is a primary enabler of influence operations and activities in the cognitive dimension that seek to affect target populations and win their support. While it will be important to keep critical electromagnetic infrastructure in operation and guarantee the population's access to the Internet of Things, this must be reconciled with the potential use of the electromagnetic spectrum by an adversary. Consequently, efficient planning and management of the electromagnetic spectrum will be required from the beginning of an operation to ensure the effective development of operations, as well as contributing to a positive perception, or at least not rejection, of friendly forces by target audiences.

Understanding the actors.

3.14. Within the hybrid warfare environment there will be many actors seeking influence, friction or harm. Some will be internal and supported or networked to external groups or states, others will be wholly external but with links to internal groups. Consider non-traditional actors such as large multinational companies which may have interests in a situation or area of operations. Breaking these down further can assist in understanding the inadvertent, or accidental, actor, where paths may collide, the competing actor, seeking to cause friction or pressure in decision making or the malign actor, who seeks to cause harm. They need to be included in the understanding; information on them, such as capabilities and intentions, will be provided by the right stakeholder group. For example, law enforcement agencies may provide the best, but alternative, view from the military

[36] Mosul Study Group*, What the Battle for Mosul Teaches the Force*, 2017, page 22.

perspective on how to deal with an armed insurgent group that obtains weapons smuggled into the country by criminals.

3.15. Whilst there will be much known about the various actors, there will also be unknowns. These unknowns need to be actively addressed and others may very likely have the answers. It is likely that there will be undiscovered activities as not everything creates a visible effect, some may be longer-term shaping or enabling to create conditions for the decisive action that is above the detection threshold.

There are many examples in history where large corporations have either overwhelmed states or have had excessive influence due to business interests. For example, the British East India Company in India, United Fruit in Guatemala in 1954 or the role of the Anglo-Iranian Oil Corporation in the overthrow of Mosaddegh in Iran in the 1950s.

3.16. An honest self-appreciation of friendly forces is important. Unconsciously, thinking is bounded by experiences, culture and values, which can lead to a skewed understanding.[37] Being self-aware of this is the first step to addressing potential cognitive biases and accepting that others who suggest something unexpected, unconventional, inexplicable, unpalatable or what appears nonsensical have merit and need listening to. It will also help in developing understanding of an adversary's motivation. It is necessary to have a very clear and honest appreciation of your vulnerabilities from your perspective. Equally as important is to ensure that you review yourself from the Emic perspective of an adversary using their psychology as this may reveal different perceived vulnerabilities and may help explain why they are targeting what they are.

3.17. Having a particularly thorough understanding of your adversaries is essential. Things that are not important to us may be very important to them in shaping how they view the world and how they believe they should interact with it. While understanding the politics, military capability and economy is standard for military planners, what may be less familiar areas are the cultural and historical aspects. Taking time to really understand them will be time very well spent. Engaging cultural and history experts may be necessary as they will provide the depth of information but also a different perspective. Listening to an adversary is also useful as it helps us understand what they may do next, as often they may start messaging about history and geography based on a historic pretext which may indicate future intentions. Such messaging may be used to gauge international opinion; no response may be interpreted as international consent.[38]

[37] Lundqvist, S., 'Why teaching comprehensive operations planning requires transformational learning'; *Defence Studies*, 15:2, pages 175–201.

[38] Ferris E., 'Forget About Hybrid Warfare; Listening to Russia helps us predict their actions'; *RUSI Wavell Room* Podcast, 18 July 2019.

3.18. The use of proxies by adversaries in hybrid warfare presents interesting challenges. Both state and non-state actors undertake hybrid warfare through proxies and time should be taken to study their methods and motives as this will reveal ways to deal with them. Methods need to be further explored by instruments of power, with previous activities examined for any trends or patterns that might provide early warning of activity. The strengths of proxies are also their vulnerabilities. For example, as they are designed to be non-attributable, they could be dealt with in a more direct manner without the risk of escalation as deniability will no longer be possible.

3.19. Corruption is endemic in certain parts of the world and may be actively encouraged by adversaries. This issue will require serious consideration of how to deal with it. Whilst a pragmatic approach will almost certainly deal with the problem in the short term, it will only make things worse in the longer term and there is a need to maintain an ethical position. Corrupt individuals will be those in positions of power or authority and likely to be the very people instrumental in creating or solving some problems. Personnel will need to be educated about the risks involved and how best to deal with them.

Part 2 – Organization considerations

3.20. Organization considerations are those that support the ability of a team to operate more effectively when faced with a hybrid warfare challenge. Creating an effective organization should presents as few vulnerabilities as possible to an adversary.

Organizational design

> 'By choosing who decides and by designing processes influencing how things are decided, the executive shapes every decision made in the unit.'[39]

3.21. Organizational design will need to be reviewed to ensure it is robust enough to remain effective under potentially novel stresses presented by hybrid warfare. The ability of adversaries to escalate their activities horizontally and vertically in different domains can exacerbate some of the characteristics of traditional military organizational structures that emphasize hierarchical, vertical workflows, centralized decision-making and strict adherence to standard operating procedures. Such structures may not be ideal to align cross-functional teams from multiple stakeholders to effectively produce the situational awareness and understanding necessary to effectively counter hybrid warfare.

3.22. To mitigate informational stovepipes, sluggish communications and delayed decisions, commanders and staff may need to consider alternatives to traditional organizational design. New organizational structures must be designed in a manner that

[39] Galbraith J., *Designing Organizations: An Executive Guide to Strategy, Structure, and Process*, San Francisco: Jossey-Bass, 2002, page 6.

contribute to the development of shared situational awareness and understanding across not only the military instrument but also with other stakeholders. Structures may be a combination of traditional hierarchical chains of command and more non-traditional matrixed or networked teams. These structures may appear inefficient and will require maintaining, but they should increase overall situational awareness and effectiveness. Commanders and staff should be prepared to create and/or shift work teams as the situation dictates, creating informal, multi-disciplinary teams empowered with decision-making authority to be responsive. The emphasis within the organization should be on collaboration as opposed to simply on coordination.

3.23. Organizational culture will also require a review. Flexibility and adaptability will be necessary components of any effective counter-hybrid warfare strategy given the tendency for shocks, surprises and innovation by adversaries.[40] However, for counter-hybrid warfare to succeed, it must be reinforced with a match in organizational culture.[41] To prepare for a counter-hybrid warfare campaign, commanders and staff should ingrain flexibility and responsiveness of thought and deed into their organization's culture.

Challenge and test

3.24. Emphasis in the organization should be placed on critical thinking, problem-solving and collaboration. Personnel must be willing to share ideas and opinions without fear of negative consequences, this will require high levels of team and interpersonal trust. All team members, including the commander, should be willing to undergo appropriate criticism, consider alternative perspectives and have beliefs and knowledge challenged. Personnel should be encouraged to develop their listening and communication skills, as well as their emotional intelligence. This may prove challenging in military organizations accustomed to formal direction and guidance in line with traditional hierarchies.

3.25. Promoting critical thinking, flexibility and innovation within an organization must go hand in hand with developing a culture of experimenting, learning and iteration. The organization must be willing to examine its activities to making constant improvement and develop fast feedback loops that are focused and disciplined to ensure observations are transformed into lessons learned as efficiently as possible.

3.26. Given the complex nature of hybrid warfare, the need to think differently and possibly adopt new ways of working, frequent exercising and experimenting is more important than ever. It will allow military personnel to become more acquainted with and evolve new tools, processes and thinking skills and allow them to build relationships with

[40] MCDC *Countering Hybrid Warfare*, 2019, page 20.
[41] Daft, R. and Armstrong A., *Organizational Theory & Design*, page 360.

the diverse stakeholder community necessary to be successful.[42] **E**xperimentation allows participants to take risks, better understand and anticipate the challenges and consequences of decisions. It will also identify any new policies and permissions necessary to make any response to an attack as effective as possible.

3.27. The value of an effective red team to properly stress test plans to understand weaknesses and discover vulnerabilities cannot be emphasized enough. A properly empowered, thinking, diverse and well-trained red team seeking to win will discover vulnerabilities in plans and processes and push any team to think differently. It is recommended that red team personnel should not form part of the chain of command of the organization being tested to prevent any conflict of interest. A hybrid warfare red team must be diverse, prepared to push boundaries and should seek to win.

Japanese war game for attack on Midway

During World War 2, at the war game for the Japanese capture of the Midway Islands, the Imperial Japanese Navy (IJN) Red Team deployed United States (US) carriers against the Japanese fleet, sank four carriers and beat them. The IJN chain of command rejected that possibility and re-ran the game, where they won. In reality, the US Navy deployed exactly as the IJN Red Team, sank four IJN carriers and won the battle.[43]

The right staff

3.28. Hybrid warfare can present many new individual and group challenges as it involves the adversarial use of both new and existing means to target societal functions in innovative ways. Hybrid warfare may incorporate deception or disinformation amongst others, all likely designed to fall below thresholds of detection, making individual hybrid warfare events difficult to understand in isolation.[44] Furthermore, these hybrid applications may involve a wider range of actors than traditionally considered by the military. Combined, these characteristics of hybrid warfare can push military personnel and organizations out of their comfort zones, possibly stymieing any response. A well-prepared staff will lessen the impact of hybrid warfare on their ability to function.

3.29. A principal characteristic of hybrid warfare is the ability to exploit ambiguity and detection thresholds, creating uncertainty and thereby reducing the ability of organizations

[42] Lundqvist, S., 'Why teaching comprehensive operations planning requires transformational learning', *Defence Studies*, 15:2, pages 175–201.
[43] Parscall, J., and Tully, A., *Shattered Sword: The Untold Story of the Battle of Midway*, University of Nebraska, Potomac Books, 2007, pages 60–63.
[44] Sebastiaan Rietjens, 'A Warning System for Hybrid Threats – is it possible?'.

to understand the problem and make appropriate decisions. For personnel trained within a traditional approach to military, or military-related, threat activities, this may be frustrating. Planning teams need to be especially close-knit and trusting of each other because the challenges created by hybrid warfare may disrupt the cohesion and effectiveness of any team responding to them.[45] Ideally, planners should be:

- self-aware;[46]
- creative, agile thinkers who embrace original ideas;
- able to adapt experience and knowledge to new situations;
- emotionally intelligent;
- socially competent;
- strong at interpersonal communication;
- open to new experiences;
- comfortable with uncertainty and ambiguity;
- physically and mentally resilient; and
- willing to experiment, make mistakes and learn from them.

3.30. In addition, there are several other attributes which may benefit commanders and senior staff who will lead, manage and coordinate personnel and activities in a hybrid warfare environment. These include:

- initiative;
- inclusiveness and willingness to collaborate;
- ability to delegate;
- a desire to be engaged; and
- comfort with professional criticism.

3.31. As discussed earlier, military personnel are products of their environment and have frames of reference which they tend to use to problem solve. These frames of reference can be 'charged with emotion'[47] leading to a rejection of alternative viewpoints that challenge them. This in turn can lead us to draw biased conclusions. Personnel will need to undergo transformational learning whereby they understand their frames of reference, what they know and how they know it if they are to succeed in a complex

[45] Staff need to be aware that this could come in many traditional forms such as blackmail, threatening family members and so on but also via new mediums such as social media.
[46] *The Red Team Handbook*, page 23.
[47] Lundqvist, S., 'Why teaching comprehensive operations planning requires transformational learning', *Defence Studies*, 15:2, pages 175–201.

adaptive system. There is a need to accommodate a broader understanding drawn from others as well as accepting that the environment is no longer linear.[48]

Resilience

3.32. One of the principles of deterring a hybrid warfare adversary is resilience. Broadly, resilience can be defined as, '…the capacity to withstand and recover from challenges, pressure, or stressors'[49] and can be present at the individual, team, and organizational levels, although in different ways.

3.33. At the individual level, resilience is a function of how quickly and completely personnel can recover from severe stress, whether short-term crises or long-term challenges. Individual resilience may be enabled by multiple sources, including personal psychological characteristics such as a positive attitude and cognitive flexibility, as well as physical fitness and social support. To ensure that military personnel are not distracted by domestic concerns, it is important to also develop the individual resilience of family, friends and community-based support networks against the potential shocks and disruption that could come from hybrid warfare.

3.34. While individual resilience is important within teams and the overall organization, group resilience is more than the sum of the people. In addition to the components that enable individual resilience, team resilience is also affected by communication, leadership, shared vision and understanding. Group resilience, whether at the team or organizational level, can also be negatively impacted by additional factors, such as lack of control, interpersonal conflict or insufficient resources. There are, however, several actions that commanders and staff can put in place to develop organizational resilience before, during and after stressful events.

3.35. Pre-crisis behaviours that can help augment group resilience includes situational understanding of current readiness, tracking of vulnerabilities (such as resource availability or access to expertise) and identifying early signs of a crisis, which involves ensuring that warnings are not dismissed prematurely. Pre-crisis is also the time for commanders and staff to mitigate vulnerabilities, identify back-up responsibilities, and develop standard operating procedures that will carry the organization through a crisis.

3.36. During a crisis, commanders and staff will rely heavily on what was put in place beforehand. Challenges and changes need to be assessed quickly, all team members need to be aware of changes and stress points, identifying what is not working and making adjustments. Team members should be monitored for overload, encouraged to ask for

[48] Ibid., pages 175–201.

[49] George M. et al., 'Team Resilience: How teams flourish under pressure', *Organizational Dynamics*, 44, 2015, pages 176–184.

assistance and supported as required. In addition, the team should be ready to defer to relevant expertise and to reach outside the organization for assistance, if required.

3.37. After a crisis, commanders and staff should quickly try to regain situational awareness by clarifying how the situation may have changed, while simultaneously establishing the status of team members. Team debriefs to identify lessons should be a regular occurrence and include follow-ups to ensure that recommended changes are implemented. Any changes should be incorporated and tested to ensure that they are robust, noting that changes to rectify previous problems might not be what is required for future ones. Openness in these ‘wash ups’ will be critical to future success.

Part 3 – Operating considerations

3.38. Operating considerations are those that an organisation might want to adopt as part of its ways of working in preparation for a hybrid warfare event. These should not become part of everyday ways of operating not implemented once an attack is detected.

A comprehensive approach

3.39. Any response to a hybrid warfare must adopt a comprehensive approach.[50] Within any cross-government response, or in pre-emptive planning, the military will most likely not be the lead department. Instead, the military must be prepared to support the decision-making of other institutions and even be part of a multinational, interagency approach. However, a military does bring structure, process and resource that most other government departments lack. Consequently, planning staffs need to be prepared to integrate other organizations into their process, possibly including business and other private sector entities. This will strengthen plans by harnessing diverse perspectives, which will increase understanding and should aid problem solving. This should become the normal way of working when planning against these threats. Planners should expect personnel from other organizations to have no understanding of the military planning process or they may conduct a different one; this offers opportunities to learn and improve. Ideally, such frictions will have been identified beforehand through experimentation and exercising, making integration easier.

3.40. When providing a solution to a problem, a military one may not be the best as civilian organizations may have greater expertise to resolve an issue; trust and cooperation between government departments must be developed. Particularly important is inter-agency planning and leadership through influence, advice and informal

[50] Finland, Norway and Sweden all have good examples of total defence policies. Norway's Total Defence and Sweden's Civil Preparedness.

followership, which is built upon individual networks and relationships.[51] Measuring performance and effectiveness using traditional military tools may prove challenging. Using a multi-agency approach to inform those tools should make understanding effectiveness and performance easier. Many of these agencies will have greater experience of what effective looks like in non-military environments. They will also be aware of, and able to access, non-traditional sources of data and information that will give a greater understanding of the impact of hybrid warfare or any actions carried out to counter these events. A comprehensive approach to conflict termination planning should anticipate where and when this may happen and allow for the preparation of plans for it.

3.41. As a whole-of-government activity, countering hybrid warfare relies mainly on non-military tools. Therefore, forming a countering hybrid warfare strategy and developing much of the whole-of-government institutional machinery – the processes, mechanisms, people and skills needed to synchronize and collaborate across government – will largely lie outside the military instrument of power. That said, the military must have input into, as well as a complete understanding of, how the strategic approach intends to maintain capacity for independent action to dissuade, deter, disrupt or prevent an adversary from carrying out future hybrid warfare. This input into the development of a strategic approach will ensure that the military can play a full part with assigned resources and ensure its approaches at the strategic, operational and tactical levels are aligned.

3.42. Commanders and staff can enable the defence contribution to an effective whole-of-government countering hybrid warfare strategy by improving the ability of the military to coordinate across government and between nations. While there is an organizational structure aspect to this issue, there is also a decision-rights aspect as central decision-making bodies – and the personnel who represent their respective organizations – must have the delegated authority to implement countermeasures quickly in a crisis.[52] Similarly, military organizations can increase their own agility to respond to hybrid warfare events by delegating authorities and decision rights to the lowest levels possible, which in some cases, may be associated with ‘flattened’ organizations. At the same time, even the most successful tactical actions will not be enough to deter a hybrid warfare adversary if those actions are unaligned with the overall policy and strategy. Even as commanders and staff emphasize delegated decision rights, they should also ensure the situational awareness and understanding of their subordinates, so they understand how to contextualize the commander’s intent to the unique hybrid warfare circumstances they face.

[51] For further Information on challenges for future military leaders, see MCDC Project *Future Leadership*, 2019.

[52] MCDC, *Countering Hybrid Warfare,* 2019*,* page 66.

A theory of success.

3.43. To counter hybrid warfare successfully it is necessary to have a realistic theory of success. Do not expect to achieve a stunning success, rather it may be through marginal gains through a series of responses and counter-responses that advantage over an actor is achieved and they are persuaded to desist from an activity. This is due to the uncontrollable nature of a complex adaptive system but also the key tenets[53] of hybrid warfare making attribution challenging and subsequent military action difficult to justify.

3.44. Advantage is achieved over an adversary by using all available instruments of power in a coordinated manner across all domains. It is best to adopt a plan that will allow opportunities for a hybrid actor to cease their activity and return to normal relationships with as little loss of face as possible. Planners need to be prepared for the hybrid adversary to rapidly change its strategy in response to their actions.[54] Continuous monitoring of the environment will increase any chances of detecting when your responses are having an effect and if it is necessary to scale back or increase activity in different areas of the MPECI spectrum to keep the pressure on a hybrid warfare adversary. The effects used should aim to influence behaviours not destroy.

3.45. Planners should always consider carefully how, when and especially what kind of military response should be used. An adversary may seek to force its opponent into a response that is not justified in the eyes of the international community, its domestic audience or depletes resources. All of this could be exploited by the adversary's narrative or used to degrade a country's ability to respond to a subsequent military attack.

The centrality of influence.

3.46. Strategic communications (StratCom) is the process by which we understand the information environment and then, based on political direction, develop a strategic narrative. This narrative is then used to give direction and guidance for all activities across the military or government. When developed as part of the StratCom process a narrative is a written or spoken account of events and information, arranged in a logical sequence. This is then used as an overarching 'story' to orchestrate activities. It describes where we are, where we are going and how we want to get there. From this narrative, effects and objectives can be developed which enable planning. To ensure coherence across all of the military's activities, guidance should be issued through a StratCom framework or StratCom Action and Effects Framework (SCAEF). This is to ensure that a state's actions communicate to audiences in a manner which creates the effects and achieves the outcomes they seek.

[53] Gradualism, ambiguity, deniability and deception.

[54] Planning staff need to be aware of this and prepared to cease a particular activity in order to pursue another one. This may call for a dynamic response from them and consequently a less-polished product.

Assessment and reviewing.

3.47. Refreshing understanding via ongoing assessment is important as the complex nature of the hybrid warfare environment makes achieving final understanding impossible. Detecting a hybrid warfare event is reliant upon constant monitoring of the environment to understand what normal looks like. This may allow the detection of indicators and warnings that something is happening and discovery to help gather the right information and interpret it correctly to identify a hybrid warfare event.[55] Initial understanding will help inform the what, where, when, why and how of monitoring and discovery which could range from indicators of domestic turmoil in nations to the rhetoric in a malign actor's social media messages; interpreting them requires a deep understanding. A monitoring and discovery regime needs to be constructed that supports timely and informed decision-making.

Response thresholds in hybrid warfare.

3.48. There are many different types of thresholds and this is one of the reasons why decisions that cross thresholds can be more difficult to control, manage or exploit successfully than optimists initially expect.[56] Some thresholds are symmetric;[57] that is, either side in a conflict might cross a threshold that is viewed similarly. In other cases it is not; a threshold may be obvious for one side but may be obscure or invisible to the other. Ultimately, all thresholds are socially constructed and are cognitive rather than physical. As thresholds are defined cognitively, they are particularly vulnerable to hybrid warfare. An adversary may focus on the manipulation of perceptions and emotions and creating ambiguity over the clarity of thresholds, although this risks accidental escalation.[58]

3.49. One way to establish thresholds for adversary actions and plan counter-hybrid warfare methods is to create dilemmas for the opponent. This means to use an indirect approach to develop own courses of action (COAs) and to create desired effects and actions. Planners should carefully study what are the possible ends and especially ways and means the opponent is trying to use. By creating dilemmas for an adversary, it might be possible to prevent hybrid warfare. For example, friendly countries, states or institutions might create a threshold to deter against possible hybrid warfare. It might be possible to create a public information campaign in different media formats for that purpose. Clearly signalling that any hybrid warfare attack against a nation's institutions may lead to

[55] MCDC, (2019), *Countering Hybrid Warfare*, 2019, page 26.

[56] Schelling. T, *Arms and Influence*, 1966, pages 153–168 and 283–286.

[57] Morgan F. et al, *Dangerous Thresholds Managing Escalation in the 21st Century*, Rand, 2008, discusses in depth thresholds and escalation in conventional and irregular scenarios. https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG614.pdf

[58] Escalation dominance theory in the nuclear domain recognized this early on during the Cold War to avoid unintentional escalation through misunderstandings of the adversary's thresholds.

countermeasures, such as economic sanctions, which may cause an adversary to think twice before carrying out their attack.

3.50. Attribution is the process by which an actor is identified as being responsible for a hostile act and this can be done internally or publicly. For public attribution to be effective, consideration should be given to releasing intelligence that could be considered as credible and convincing evidence.

Thresholds, Ambiguity and the Skripal Case, 2018

On 5 September 2018, UK authorities identified two Russian nationals as being suspected of the poisoning of Sergei Skripal, a former Russian military officer, and his daughter Yulia in Salisbury, England on 4 March 2018 using a Novichok nerve agent. This incident highlights several attempts to create ambiguity over appropriate response thresholds. The Russian nationals attempted to stay below the threshold of detection but once the attack was detected efforts were made create ambiguity over a decisive response by the UK. This included Russian Foreign Minister Sergey Lavrov rejecting the UK's claim of Russia's involvement in Skripal's poisoning and accusing the UK of spreading 'propaganda'. Lavrov said Russia was 'ready to cooperate' and demanded access to the samples of the nerve-agent used to poison Skripal. The request was rejected by the UK government. The multiple Russian narratives were designed to create confusion and ambiguity in the minds of policy-makers and target audiences.

Deterrence and hybrid warfare adversaries.

3.51. Countering Hybrid Warfare 2 identified deterrence as one of the most effective tools to counter a hybrid warfare threat.[59] Importantly, while hybrid warfare complicates traditional approaches to deterrence, it does not fundamentally change the range of deterrence options. In other words, hybrid warfare adversaries can be deterred, although the application of specific deterrent measures must be updated to account for the evolving characteristics of hybrid warfare. Deterrence theory has three pillars.[60]

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

[59] MCDC, *Countering Hybrid Warfare*, 2019, page 35.

[60] Ibid, Chapter 4. A more detailed description of deterrence theory and how it is complicated by hybrid warfare see.

3.52. Deterrence strategies that look to deter an adversary, either through denial or punishment, seek to either undermine an adversary's ability to achieve their objective in the first place, or convince them that the retaliatory costs of achieving their objectives are prohibitive. In both cases, the effectiveness of each becomes more complicated in a hybrid warfare environment. For example, the credibility of retaliatory deterrence in the cyber domain is complicated by the challenges of attribution.[61] Like most other aspects of hybrid warfare, there is no solution for all situations; however, practitioners can be guided by several principles.

- Traditional deterrence remains vital and may even need to be strengthened.
- Hybrid warfare aggressors are deterrable.
- The pillars of deterrence remain effective but must be adapted for hybrid warfare aggressors.
- Resilience is important, but not everything.
- Effective hybrid warfare deterrence strategies must be tailored to the aggressor and the situation.

Planning for effective deterrence against hybrid warfare adversaries.

3.53. While deterrence of hybrid warfare adversaries should be viewed as a whole-of-government activity versus that of a single instrument of power, there are practical steps that military planners can take which will improve their ability to support deterrence strategies. Planners should be aware of the overall governmental framework to coordinate deterrence measures and support the development of countermeasures.[62] Beyond that, planners should think about and understand how to disaggregate an adversary's strategies to identify opportunities for tailored and targeted deterrence measures, but also how an aggressor will potentially interpret a deterrer's actions.[63]

3.54. From a preventative standpoint, developing denial capabilities, such as hardening Information Technology (IT) infrastructure or increasing the resilience of supply chains, will continue to be important, as will maintaining conventional capabilities that may be used for deterrence by punishment. However, it is important to note that deterrence measures can have unintended consequences. Hardening a target in one area may simply cause an adversary to focus their efforts elsewhere, and that may be an area that poses even greater difficulties.[64] Similarly, it is important that military planners do not simply prepare to deter the last attack. Hybrid aggressors should not be underestimated and each attack will

[61] Emily Robinson, *Hybrid Warfare and Deterrence*, DRDC Canada, 2017, page 4.

[62] MCDC, *Countering Hybrid Warfare*, 2019, page 68.

[63] MCDC, Countering Hybrid Warfare Project, *Can hybrid attacks be deterred? And if so, how do we do it?* 2018.

[64] Ibid.

almost certainly be different from the last. In conducting deterrence against hybrid warfare there is a very realistic chance that miscalculation could occur due to a failure to understand an adversary properly and what they are likely to do vice what you believe you would do in such a situation. Mirror imaging is important to understand.

3.55. As with other aspects of hybrid warfare, military planners must be comfortable with uncertainty. This is because it will likely be difficult to measure success since proving why something **did not** happen – which is the goal of successful deterrence – is more difficult than proving why it **did** happen. To that end, planners should strive for creativity when developing measurement tools to assess effectiveness of deterrence measures.

Part 4 – Planning tools considerations

3.56. There are several tools that complement the operations planning process. Analytical tools, such as centre of gravity (CoG) analysis, comprehensive preparation of the operating environment (CPOE), operations assessments and risk evaluation all assist critical thinking regarding specific portions of the planning process. Knowledge management tools, such as synchronization matrixes and information collection plans, facilitate the processing of vast amounts of information, as well as the representation of key deductions, comparisons and conclusions to others. Lastly, situational awareness tools, such as tools for operations planning functional area service (TOPFAS) or a joint common operational picture (JCOP) can help develop organizational shared understanding and complement key operational activities like real-time alerts and warning.

3.57. Like the overall planning process, these planning tools remain applicable to hybrid warfare. However, for their potential to be maximized, these tools may need to undergo slight modifications to be more aligned with specific characteristics of hybrid warfare; this will only be realised by experimenting to see what works. For example, many of these tools are already designed and employed within a comprehensive approach to operations, including the need to work collaboratively with non-military stakeholders. At the same time, implementing a counter-hybrid warfare approach may require this collaboration to go even farther, partnering not only with representatives from other instruments of power and non-governmental organizations, but also the private sector. In fact, in countering hybrid warfare, the ability to incorporate private sector expertise in a variety of domains has the potential to be a critical enabler, particularly cyber.

3.58. In some cases, these tools will need to be modified for a counter-hybrid warfare approach all in the same way, for example, all of the tools will benefit from greater collaboration with others to develop them. In other cases, modifications may apply more to one suite of tools than another. As with most aspects of countering hybrid warfare, there is no generic solution, and commanders and staff are encouraged to think creatively about bespoke solutions, guided, where appropriate, by the following considerations.

Analytical tools.

3.59. This category of tools assists in the detailed examination of specific topics, often by breaking that topic into smaller parts. CoG analysis, for example, identifies an actor's principal source of power by looking at critical capabilities, critical vulnerabilities and critical requirements. For these tools to be effective, practitioners must be able to draw upon a solid base of knowledge, as well as an understanding about how characteristics of hybrid warfare may affect the application of that knowledge. For example, traditional CoG analysis has focused on the identification of fixed, primarily military, CoGs. In a counter-hybrid warfare approach, adversaries may have multiple, relevant, non-military CoGs. Furthermore, primacy may shift among them in a flexible and dynamic manner, as illustrated in Figure 5. This will have clear impacts on the development of operational designs, likely increasing the need for flexibility and adaptability. To remain useful, CoG analysis may need to be modified to incorporate this characteristic of hybrid warfare.[65]

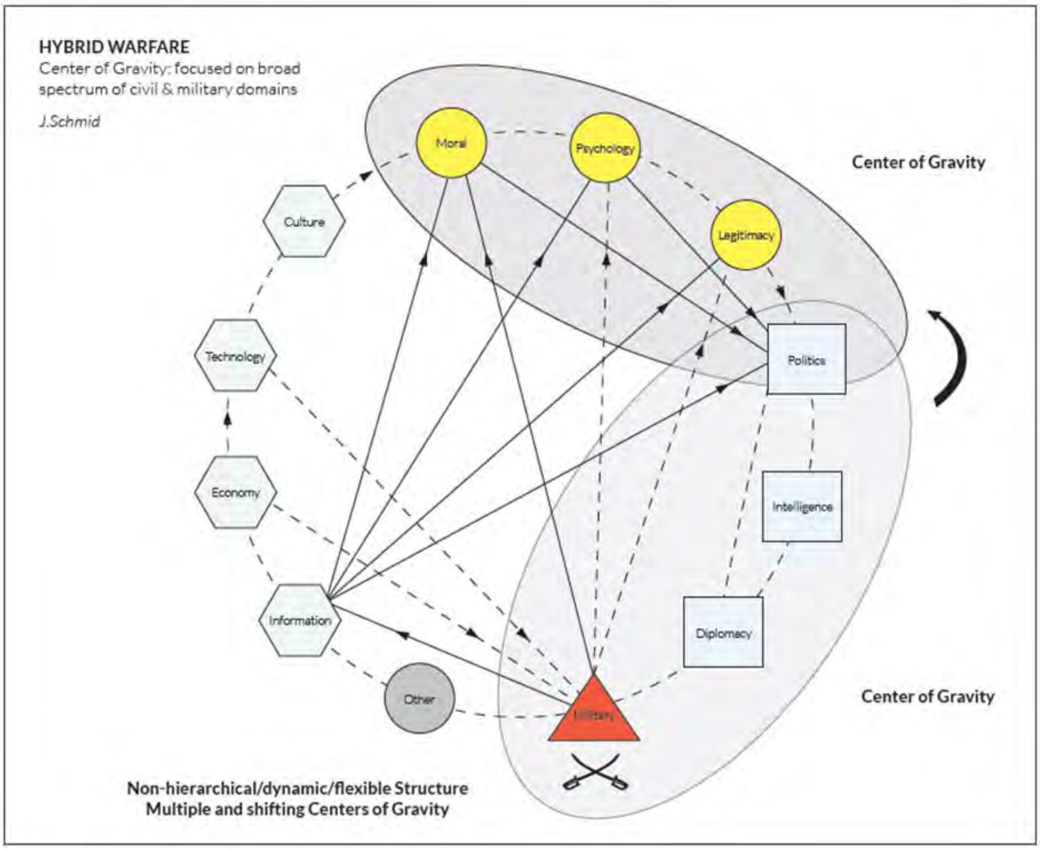


Figure 5 – Multiple centres of gravity in hybrid warfare

3.60. The use of analytical tools must be conducted with an awareness of how new technologies have increased both the possibilities for hybrid warfare, but also the numbers

[65] Hybrid Centre of Excellence paper on CoG analysis. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-84/jfq-84_86-92_Reilly.pdf

of potential actors. In hybrid warfare, it is possible that the manifestation of power may differ from traditional experiences, with relational power displacing resource-based power as an indicator of influence. Thinking critically about these developments in the operating environment, and how they affect application of these analytical tools will be a necessary step to ensure success of operational plans.

3.61. Several best practices will facilitate this critical approach to analysis. Incorporation of subject matter experts wherever possible will increase the depth of the analysis. Likewise, having diverse representation among practitioners will encourage the incorporation of a variety of perspectives. This category of tools will also benefit greatly by the inclusion of a challenge function, such as that provided by alternative analysis. Lastly, as technology advances, it may be possible to harness artificial intelligence and machine learning to help process large amounts of data and enhance planning. This type of assisted analysis has particular potential for data rich areas and should continually be investigated and improved.

What is alternative analysis?

Alternative analysis is the deliberate application of independent, critical thought and alternative perspectives to improve decision-making. It consists of several thinking methods and techniques that can help stimulate creative problem-solving processes at any stage, from problem identification to solution implementation. These techniques vary from those that can be used at an individual level with little preparation to those designed for facilitated group discussions. If properly enabled, alternative analysis is a powerful problem-solving tool that can enhance the ability of commanders and staff at all levels to think 'outside-of-the-box' when operating in a hybrid environment.

Knowledge management and situational awareness tools.

3.62. This category of tools, which help collect, assess and share information, are affected not only by aspects of hybrid warfare, but also by developments in the information environment. There is a greater amount of information available, and the primary actors in the information environment are changing. There is also a greater amount of disinformation, which people and organizations are generally less capable of spotting. Furthermore, the quality of some sources, such as traditional media, is decreasing whilst the number of actors, for example bloggers or micro-influencers who may not subscribe to professional standards, is increasing. Therefore, these tools need a greater ability to discriminate and assess than was previously the case.

3.63. Along with greater amounts of information and a greater number of stakeholders, there is a need for more efficient and effective information fusion. Here, again, the tools must consider the latest developments in artificial intelligence and machine learning to enhance the ability to gather, process, exploit and distribute information. Military organizations should consider investing in information processing capabilities and skills, which can be used to develop a base of knowledge which includes an understanding of what normal looks like.

3.64. Lastly, given the dynamic nature of hybrid activities, knowledge management and situational awareness, tools must have built-in resilience and flexibility to be able to rapidly identify opportunities in a changing operating environment. For example, during counter-insurgency operations in Iraq and Afghanistan, synchronization matrices tended to capture detailed time and space conclusions, extending, in some instances, for periods as long as years. This level of detail may have been possible in Afghanistan; however, it is unlikely to work against hybrid warfare adversaries in complex environments. Practically, therefore, it may be necessary to amend synchronization matrices to include greater degrees of uncertainty, where activities after certain times are indicated as possible, but not definite.

3.65. The next chapter presents a general rationale and considerations as well as key questions and actions that planners may want to consider for each section and step of Allied Joint Publication-5, *Allied Joint Doctrine for Operational-level Planning*, Chapter 4 when preparing for a hybrid warfare event or responding to one.

Chapter 4 – Planning considerations

4.1. **Introduction.** The aim of this chapter is to help the planner understand some additional advice for operations design in general and then in detail at each planning step when confronting hybrid warfare challenges. This advice is not definitive and planners should enhance it with their knowledge, experience and the advice in Countering Hybrid Warfare (CHW)1 and CHW2.

Operations design

4.2. In a hybrid warfare scenario, operations design will be even more critical to the success of any plan due to the tenets[66] and characteristics[67] of hybrid warfare, together with the effects created by hybrid warfare actors.[68] The difficulty in discovering attacks combined with the ability of the actor to rapidly alter their ways and means creates significant challenges for how to prepare and respond. Consequently, success in hybrid warfare will often look like a return to normal competition rather than defeating an adversary. This 'paradigm of success' must be borne in mind when designing operations, selecting aims and, ideally, choosing an indirect approach for possible courses of action (COAs). The structured processes that enable operations design have additional considerations when planning for operating in a hybrid warfare environment.

Ends, ways, means and risks

4.3. **Rationale and considerations.** The ends selected must be achievable whilst avoiding an overwhelming effect on an adversary; destruction is often not possible due to the levels of justification necessary in an ambiguous situation. Therefore, the cumulative effect created by influencing an adversary's behaviours through coordinated, cross-governmental physical and non-physical actions to achieve marginal gains is often more effective and realistic. The desired end state is likely to be to influence an adversary to cease their activities and return to normal competition. The ways and means selected should support this whilst being mindful of the potential second and third order effects. The foreseeable risk in all of this is that the adversary will change their strategy, which will have to be detected all over again and ends, ways and means reselected. This risk must be assessed in relation to the actions and desired effects, as it will force an intelligence and information collection cycle to maintain a current view of the situation.

[66] Gradualism, ambiguity, deniability and deception.

[67] The combined use of multiple instruments of power to create asymmetric effect through targeting an expanded range of vulnerabilities; a synchronized attack package that exploit both horizontal and vertical axes of escalation; an emphasis on creativity and ambiguity to create synergistic effects (including in the cognitive dimension).

[68] That are based on the following three interdependent elements: (1) critical functions and vulnerabilities; (2) synchronization of means; and (3) effects and non-linearity.

Key questions and actions

The following key questions and actions should be considered.

- Do the ways and means used achieve the ends of dissuading the adversary from continuing with their strategy and returning to normal competition?
- Is the focus on those elements of an adversary's strategy that will achieve marginal gains and dissuade them from continuing with their strategy?
- Are the ways to influence an adversary properly understood?
- Are the advantages of marginal gains, rather than a decisive blow, fully understood and assessed against a possible adversary change of strategy?
- Are you using the right subject to assess the second, third order impacts?

Understanding the operating environment

4.4. **Rationale and considerations.** A thorough understanding of the operating environment is critical to success in hybrid warfare. Among the most important things to understand are the different actors and audiences, their sensitivities and perceptions of the situation and how they can be influenced, as well as the effectiveness on them of any influence campaign. The extensive and decisive use of the instruments of power in all domains by all actors, with special attention to the use of the information and electromagnetic functions, will require a multi-domain approach to understand. The ends, ways and means employed by third party actors could provide pivotal support and facilitation of the adversary's strategy and any indirect actions. Finally, the desired conditions and associated actions and effects and what these mean to the different actors and audiences as well as the impact on the infrastructure and non-physical domains all needs fusing to understand the totality of interactions.

Key questions and actions

Understanding the operating environment.

- Do we have experts on the different instruments of power?
- Do we have experts on the different actors and population sensitivities?

Factor analysis and key factors.

- Analyze the adversary’s use of the cyber domain and the civilian population’s access to it.
- Analyze the use of mass media and social networks by the adversary and any narratives to influence different audiences, especially those with a tendency to disaffection.
- Assess the effect of the adversary’s actions on our population.
- Monitor actors to identify changes in their ends, ways, means and systems of relationships.
- Have an honest understanding of yourself and the adversary.

Desired conditions.

- Are the conditions of the desired final operating environment and that of each of the actors present in the area of operations (AOO) and area of interest (AOI) clearly defined?

Operations design concepts

4.5. **Rational and considerations.** Traditional operations design concepts will require additional considerations when considering hybrid warfare threats. The selected end state should be one that provides an acceptable resolution not only to the adversary but to all actors in the AOO, allowing a return to pre-attack levels of normality and acceptable interstate competition. The restoration of critical infrastructure and access to functions such as the electromagnetic spectrum is crucial to ensure the return of normal competition between actors. Operational objectives ideally should be achievable without the need for the overwhelming use of force. Consideration should be given to the welfare and opinions of the civilian population in the AOO as well as the international community's view of the objectives, and also how an adversary may manipulate them to influence your campaign.

4.6. The adversary’s centre of gravity (CoG) and those of the different actors should be influenced by an indirect approach to reach the decisive conditions through the synchronized use of the instruments of power against a target’s critical vulnerabilities. Many of the decisive conditions will probably be achieved through effects created by non-military means and in non-physical domains, but effects in the physical domains, which can be decisive, should always be planned to avoid an adverse reaction from the population or exploitation in the information space by an adversary. These actions should focus on the adversary and other actors in the AOO, seeking to disaggregate their strategy and attack key vulnerabilities and enablers by using the most effective, not necessarily the most destructive, means. Any damage to key civilian infrastructure must be repaired as soon as possible to allow a return to normal relations.

4.7. The effort of each lever of power in each line of operation (LoO) must be based on the priority of the LoO. To achieve synergy in one or several LoOs, actions using the different instruments of powers must be synchronized. By making society, infrastructure and military units as resilient as possible will avoid culmination from adversary hybrid warfare activities. Adversary culmination should be sought through the coordinated employment of physical and non-physical actions.

4.8. The sequencing and phasing of an intentional mixture of actions using all the instruments of power, across all domains, throughout the entire depth of the AOO and simultaneously along multiple LoOs, should result in achieving the decisive conditions. In a hybrid warfare environment, phases should be designed to provide different synergistic effects at the appropriate time. These effects are created by the coordinated use of the different instruments of power, according to the priority of each LoO and the supported/supporting relationships of each lever. In each phase, the commander will decide the main effort.

4.9. The hybrid warfare actor tries to impose an unanticipated and creative high tempo to their actions to seek the advantage that will secure their final goal. To counteract this activity, it is essential to constantly monitor the operating environment and be prepared to use great flexibility and capacity in decision-making and the execution of actions. The COAs must be flexible enough to adapt to the ever-changing strategies of the hybrid actor. The branches and, even more so, the sequels should look more like a series of possible scenarios which will be confirmed by means of ‘signposts’ and will lead to decision points where a series of pre-determined measures will be adopted. However, a skilled adversary will also be anticipating this and will seek to force situations that may not have been anticipated.

Key questions and actions

End state.

- Is the end state politically acceptable and will it facilitate a return to normal competition?
- Does the end state consider maintaining the necessary infrastructure for the population to continue normal life activities?

Transition and termination.

- Include among the criteria for completing the operation the commissioning of key functions for normal life.
- Develop extensive information operations to explain to the different audiences,

friendly, adversary of the international efforts to help the populations affected by the operations return to normal life.

Direct versus indirect approach.

- To act against the key actors that collaborate in the adversary's strategy.

Objectives.

- Do not destroy or permanently damage vital infrastructure for the population.
- As far as possible avoid actions that may cause population displacement.
- Promote the return to normality in the transition phase.
- Try and anticipate possible second and third order consequences of actions.

Decisive conditions.

- Consider targeting the key vulnerabilities of the actors that support the adversary’s strategy?

Effects and actions.

- Consider for use all the actions and effects, no matter the magnitude, of all the actors and instruments of power.
- Use actions from non-physical domains to create effects and to support actions from other domains.
- Creatively target the enablers of the adversary's strategy by using the most effective and acceptable means.
- Evaluate possible negative consequences of the actions, especially in the population.

Lines of operation.

- Consider in each LoO all instruments of power and actors, as well as their supported/supporting role.
- Synchronize the effects of each action in time and space for each LoO.

Culmination.

- Evaluate the resilience of friendly units, the population and infrastructure to avoid early culmination.
- Act in a synchronized manner with all means and in all domains to cause a

culmination of the adversary's means and of their population.

Sequencing and phases.

- Define by each LoO and phase the time and place required for the coordinated use of the instruments of power to create the effects necessary to reach the decisive conditions.
- Ensure there is the necessary simultaneity, sufficient tempo and depth to actions to disrupt the adversary’s rhythm and reach the decisive conditions to achieve the goal?
- Permanently monitor the operating environment to identify and react to rapid and unexpected changes in strategy and adapt current operations or branches and sequels as required.

The principles of planning remain valid when operating against a hybrid warfare threat, with some additional considerations.

- Unity of effort: are all the instruments of power integrated to ensure coherence? Have we established effective communication links with all other agencies?
- Concentration of force: against what or who? When, where and on what basis can preparations be initiated? Ensure there is capacity to concentrate physical and non-physical effects and not just from the military.
- Economy of effort: but via the combination of different tools is imperative.
- Freedom of action: how can that be ensured when it is needed?
- Defining objectives: could be more difficult in a hybrid warfare scenario. Who or what defines the scenario for the military commander?
- Flexibility: possibly the most important part in an ambiguous scenario. Who can help the military better understand and how?
- Initiative: difficult to achieve. Have you constructed a team that enables divergent thinking?
- Offensive spirit: but not necessarily in action.
- Surprise: through a comprehensive understanding of the operating environment and actively seeking to discover unknown unknowns attempt to avoid being surprised.
- Security: not only of the military forces, but also the home nation and identified interdependencies with civilian organizations.
- Simplicity: how can the plan be simple and flexible enough in a hybrid warfare environment?
- Maintenance of morale: how will the effect on the population in the homeland affect

the troops?

- How to counter hybrid warfare with own actions (time and different domains)?
- How can the effects of hybrid warfare be anticipated at all levels?
- Comprehensive understanding of the operating environment, across domains.
- Do we really understand the problem?

The planning process: Step 1 – initiation

Initiation – Initiating directive and derived planning directive

4.10. **Rationale and considerations.** The initiating directive, higher commander's planning directive, joint intelligence preparation of the operating environment (JIPOE) and other intelligence products must provide information about the instruments of power used by the adversary, any possible strategy, who the different actors present in the AoO are, the dynamics of relationships between all parties and the coordination already established with them at the strategic level. It is important that the correct information is available at this stage as this will shape outputs and any subsequent planning process. Remember that the actions of an adversary could change quickly and, consequently, the staff need to be prepared for changes in the direction of the plan.

Key questions and actions

- Has there been cross-government engagement to identify the adversary's hybrid warfare strategy and implications?
- Have the instruments of power used by the adversary and other actors been identified, with special attention to the use of the information and manipulation of the electromagnetic spectrum?
- Have all the actors, regional and international, present in the AOO been identified and are their dynamics, relationship and interests, and what this means to you, understood?

Initiation – commander`s initial planning guidance

4.11. **Rationale and considerations.** The Initial Planning Guidance (IPG) and warning order must include, at a minimum, the adversary's key vulnerabilities and any enablers for its identified strategy. This should also include any ways and means they may employ, with special emphasis on their information operations, their aims in the cognitive dimension and the manipulation of international law in their favour.

Key questions and actions

- Do the IPG and warning order contain the necessary information to understand the operating environment and the mission to be executed?
- Is the adversary's and other actors' use of the cognitive dimension, the information functional area and our perception of the law and traditions correctly understood?
- Has the establishment of relationships with the different actors present in the AOO been authorized?

Initiation – operational liaison and reconnaissance teams

4.12. **Rationale and considerations.** An operational liaison and reconnaissance team (OLRT) must contain personnel who have an excellent understanding of the planning process, hybrid warfare and the organization they will be liaising with. Ideally, they will be some of the best people and will have had numerous opportunities to meet their opposite numbers before any crisis is initiated. This will build trust and ensure they can work together and understand the contribution of others. Equally, military teams should expect to routinely see liaison personnel from other parts of government and other organizations embedded in their headquarters.

4.13. OLRTs need to be configured correctly to conduct their roles effectively. Specialists from other government departments should routinely form part of these teams and there should be a preparedness to accept subject matter experts from non-governmental organizations. The OLRT needs to be trained to conduct a whole of society review to fully understand where they may need to look to comprehensively understand what is happening.

Key questions and actions

- Does the OLRT have specialists from the different instruments of power capable of contributing to the JIPOE and other intelligence products?

The planning process: Step 2 – mission analysis

Framing the problem – strategic context review

4.14. **Rationale and considerations.** A thorough review and appreciation of the strategic aspects of a situation is needed to set the context for operational activities and, in turn, to initiate operational-level planning. Some of the most important aspects to review in a hybrid warfare environment will include the involvement and perceptions of the international community regarding the conflict, CoG assessments of an adversary and other actors, and economic factors.

Key questions and actions

- How do different actors and stakeholders perceive the strategic environment and the factors contributing to the situation?
- What is the perception of the international community?
- Have the adversary's strategy and CoGs been identified, including how they may synchronize their instruments of power?
- What are the adversary's key vulnerabilities?
- Who are the actors and proxies supporting the adversary's strategy?
- What are the CoGs of the other actors and stakeholders?
- What are your key vulnerabilities and how are they susceptible to the adversary's strategy?

Framing the problem – appreciation and refinement of the joint intelligence preparation of the operating area

4.15. **Rationale and considerations.** The JIPOE is a primary tool to ensure that situational awareness is continually updated. Traditional approaches to compiling a JIPOE are challenged in a hybrid warfare environment because hybrid warfare actors will seek to stay below thresholds of detection through unexpected actions and novel tactics; they can also be expected to suddenly change their strategy. Therefore, the JIPOE must be continually refined and adapted to account for novel hybrid warfare tactics by using innovative methods to reimagine indicator-based warning methodologies, as well as incorporating alternative warning methodologies that move beyond traditional indicators.

Key questions and actions

- Is the JIPOE being regularly updated by all stakeholders and shared with them?
- Are the intelligence products constantly examining your critical vulnerabilities across the political, military, economic, social, informational and infrastructure (PMESII)

spectrum?

Framing the problem – evaluation of actors

4.16. **Rationale and considerations.** In a hybrid warfare situation it is particularly important to have a deep understanding of potential adversaries and other actors. This includes their goals, their strengths and weaknesses, and how they employ their instruments of power. Since adversaries are often part of a larger network, it is important to analyze the components of this network to understand relationships and influences, possible proxies and potential supporting activities. This analysis will help identify strengths and critical vulnerabilities of the hybrid warfare adversary. This information must be routinely updated in the JIPOE.

Key questions and actions

- How current and extensive is the understanding of adversaries and their potential proxies?
- Has authorization been given to allow engagement with different friendly actors to better understand the situation by including their perspective? If not, has direct liaison authority been requested?

Framing the problem – factor analysis and key factors

4.17. **Rationale and considerations.** In a hybrid warfare environment, factor analysis must pay particular attention to the following elements.

- Time – the readiness and authority of decision-makers and available forces to implement countermeasures in response to the actions of an adversary.
- Space – the interdependence and overlap of physical and non-physical domains, and how the absence of clear geographical boundaries might affect delineation of the AOO, area of Influence, and AOI for the operational force.
- Force/actors – the non-military capabilities available to an adversary and what effect they might have on military operations, possible hybrid warfare tactics, techniques and procedures (TTP), or known limitations that might impact an adversary's actions, such as legislation or sociocultural factors.
- Information – the actors involved, what messages they convey and to what extent they dominate or influence in the information domain. This factor must also consider our own information operations activities and possible actions to intervene to obtain and retain advantage.

Key questions and actions

- What is the notice to move (NTM) or reaction time of available forces and whole-of-government actors? Is this enough for the perceived threat? If not, how can reaction times be reduced?
- Has the AOO and AOI been clearly defined in all domains?
- Are there any international laws or generally accepted customs that restrain or/and constrain the actions of an adversary?
- What are an adversary's information operations capabilities and how are they being used?

Analyze the mission – operational objectives and criteria of success

4.18. **Rationale and considerations.** Given the opaque nature of cause and effect in a hybrid warfare environment, it is particularly important that operational objectives and intended effects are focused on where they will have greatest effect on adversaries, such as their vulnerabilities. This must be matched with a deliberate and disciplined commitment to measure the effectiveness of our actions, which may be through innovative or non-traditional methods.

Key questions and actions

- Consider how your actions will affect the CoGs of an adversary or other actors, and what second and third order consequences may result? Are these the desired effects?
- Are there clear mechanisms to collect and analyse data to feed into measures of effect/measures of performance?

Analyze the mission – centre of gravity identification and analysis

4.19. **Rationale and considerations.** Your own CoGs must be considered when identifying any potential instruments of power that an adversary may use to be able to defend it correctly. Protecting your own CoGs is especially important to mitigate your vulnerabilities, since the adversary is likely to have the initiative and it will be very difficult to attack the vulnerabilities of the adversary CoG militarily.

4.20. Since the CoGs of all actors in a hybrid environment could change over time, LoOs and COAs must be developed with enough resilience in them to allow for plans to change (friendly and adversary) and to adopt new COAs, branches and sequels.

4.21. More broadly, when identifying all critical capabilities, any analysis must consider:

- how the adversary will act in the cognitive dimension;
- any critical infrastructure and its resilience to cyber or physical attacks;
- the ability to establish and use information networks;
- the population's resilience against influence operations;
- what effects could impact infrastructure or production capabilities;
- how up to date the situational awareness is;
- the ability to communicate and interact with a population before, during and after an event;
- the capability to respond to a hybrid warfare action in a timely manner and
- the ability to interact with partners and allies.

4.22. When identifying all critical vulnerabilities, special attention should be paid to:

- the degree that an adversary manipulates information and/or controls the media;
- the possible unlawful use of cyberspace by an adversary;
- the ability to boost the narrative and actions of citizens and dissident groups within an actor's territory;
- how quickly violations of international law could be exploited;
- the ability to isolate an actor from obtaining critical resources from third parties;
- actors' access to dual-use technologies;
- the susceptibility of a targeted population to an adversary's information operations and
- the degree of societal resilience.

Key questions and actions

- Does the JIPOE identify areas in which an adversary's CoGs could be affected?
- Have you identified how an adversary's CoAs might change due to their CoGs being

targeted?

- Have the adversary’s critical capabilities, in particular those related to non-physical domains, been considered?
- Have the critical vulnerabilities, in particular those related to non-physical domains, been identified?
- Are all the adversary’s breaches of international law or/and any actions against a population being exploited to isolate them?

Analyze the mission – developing assumptions

4.23. **Rationale and considerations.** There is often a lack of information available to planners in a hybrid warfare scenario because of the long-term nature of many hybrid warfare strategies, the indirect approach taken by hybrid adversaries and the difficulty of attribution. Consequently, planners will need to make frequent use of assumptions, particularly when developing contingency plans. Due to the versatility and creativity of hybrid warfare actors, assumptions should initially be kept as broad and open as possible, preserving as many options as possible and allowing events and actions to develop over time to help provide greater clarity. An updated JIPOE will assist with the confirmation or denial of assumptions and help influence decisions to execute branches and sequels.

Key questions and actions

- Have you confirmed or denied an adversary’s strategy and its use of instruments of power? Can you in turn confirm an adversary’s CoA?
- Is there enough information for operations and planning to use for, and adapt to, the evolving operating environment through branch plans and sequels?

Analyze the mission – determining critical operational requirements

4.24. **Rationale and considerations.** Since effective counter-hybrid warfare is a whole-of-government activity, it is especially important that all instruments of power are coordinated. A key enabler of this is a robust and reliable command and control structure able to reach all stakeholders in any circumstances.

4.25. To properly understand all the relevant actors in an AOO and develop effective counter-hybrid warfare plans it is critical that all stakeholders from the whole of government and more broadly are incorporated from the beginning of the planning process. In particular, planners should seek input from these stakeholders as to how they perceive conditions for success, as well as how they could potentially create effects and set the decisive conditions needed to reach objectives. In this way, the development of LoOs and COAs can lay the framework for all the stakeholders to work in concert.

Key questions and actions

- Is the command and control network robust and reliable, and does it have enough capacity to integrate other partners? If not, has the use of other technical solutions and/or liaison officers been considered?
- Have links been established with other friendly actors in the AOO? Have those actors been integrated into the planning process?
- Consider a positive information campaign aimed at the target population to prevent an adversary population unifying against the friendly actions.

Analyze the mission – determining requirements for complementary interaction with relevant international and national actors

4.26. **Rationale and considerations.** The use of non-military means to achieve operational objectives is normal in hybrid warfare and should be seriously considered.

Analyze the mission – limitations on operational freedom of action

4.27. **Rationale and considerations.** Any limitations and restrictions imposed by the political level and the operational commander should be kept to a minimum due to the ambiguous and novel nature of hybrid warfare. Ideally, they should focus on ensuring respect for the rule of law and what coordination with other instruments of power is allowed.

Key questions and actions

- Monitor the situation to avoid any action or measures that may negatively affect a civilian population's (ours and theirs) perception of friendly forces and operations.

Analyze the mission – risk assessment and tolerance

4.28. **Rationale and considerations.** Risk assessment in a hybrid warfare environment is complicated because it must not only consider physical risk but also non-physical risk, such as cognitive and cyberspace. Additionally, risk assessments must consider the second and third order effects of actions by the different actors and how these could potentially alter the situation.

Key questions and actions

- Do your COAs consider the impact of counter-hybrid warfare activities on the local population, and repercussions from the international community?
- Does the risk assessment include perspectives and mitigation measures from across all the instruments of power?

Developing the initial operations design – determining lines of operation

4.29. **Rationale and considerations.** The strategic objectives must provide planners with enough flexibility to develop LoOs that are creative and agile. In a hybrid warfare environment it is best to use an indirect approach, applying second and third order effects with the aim of attacking or influencing the adversary in an unexpected and hidden way. To do that, planners might wish to seek marginal gains by focusing on key vulnerabilities, targeting specific assets that enable the hybrid warfare campaign or increasing focus on specific, sensitive actors.

Key questions and actions

- When designing LoOs and COAs, planners might wish to consider how to achieve marginal gains through disaggregation of an adversary's strategy and disrupting key enablers with the most effective instrument of power.

Developing the initial operations design – conditions to be established and selection of decisive conditions

4.30. **Rationale and considerations.** When determining which actions will produce intended effects, it is important to identify which elements of an adversary's system can be influenced by military or non-military means and vice versa. Using coordinated actions will be important to obfuscate the origin of counter-hybrid warfare activities, thus increasing the impact on an adversary. Planners need to be aware that many of the decisive conditions may be achieved through the effects created by non-military means in non-physical domains. Planners must consider the possible effects of non-aligned actors in the operating environment and how these might influence the setting of decisive conditions. Equally, time is a critical factor to study regarding the harmonization of different LoOs, the coordination of simultaneous near and deep operations in the physical and non-physical domains, as well as execution with a high tempo to seize and maintain the initiative. Due to the ability of hybrid warfare actors to quickly adapt their strategies and method of actions, the operations design must be agile and responsive to rapid changes. This will put a premium on the need for flexibility in the execution of current operations, as well as on adapting future operations. Lastly, it is important to consider that in the initial phase of a crisis if there is no escalation then major actions may have a dissuasive character.

Key questions and actions

- Have the CoGs of any of the actors changed?
- Determine which elements of an adversary's system can be influenced by military and/or non-military means.
- Has a network been established to coordinate actions with military and non-military actors not embedded in our force?
- Have we identified which actors are supporting the military forces? How will they provide this support and what effects they will create?
- Have we targeted the key vulnerabilities of the actors that support the adversary's strategy?

The planning process: Step 3 – courses of action development

Adversary courses of action and other factors affecting course of action development – consideration/confirmation of the actions of non-adversary actors

4.31. **Rationale and considerations**. As hybrid warfare actors are typically characterized by creativity, agility and dynamic decision-making, they generally have the capability to change strategy, plans and actions to accommodate the ever-changing conditions of the operating environment to include adversary success. As a result, changes in adversarial COAs frequently occur and must be accounted for in the development of friendly COAs. Any indicators must be capable of identifying expected and unexpected threats and establish threshold values to identify any escalation of the conflict. They must also be able to detect unknown threats by observing society in a holistic manner that integrates all the powers of the nation. The actions of other actors in the operating environment, and their effects, must be considered, as a minimum and should include the following:

Key questions and actions

- Evaluation of adversarial courses of action.

  - o Has it been possible to discern the adversary’s strategy?
  - o Are the indicators established to confirm that the adversary's COA as valid?
  - o Are the assumptions used in planning to predict the operating environment confirmed?
- Consideration/confirmation of the actions of non-adversary actors.
  - o With the available information, can we deduce the actions, the instruments of power used, and the actors that create negative effects for our forces?
  - o Are the actions of the opposing actors coordinated and, if so, what instruments of power do they use?

Developing our own courses of action

4.32. **Rationale and considerations.** In hybrid warfare, our own COAs must be flexible enough to adapt to the ever-changing strategies of the adversary and respond to any change in the situation. This flexibility, along with the integral flexibility of our own military forces, will provide the opportunity to react before using branches and sequels. Flexibility must also be a factor when engaging with other friendly actors to coordinate actions in a supporting/supported role. In all cases, planners should seek non-linear effects and seek to create effects through the coordinated use of all the instruments of power.

4.33. Effective counter-hybrid warfare strategies put a premium on the operation assessment process to check that plans are achieving their intended objectives and, if required, adapt current operations through branches and sequels. Due to the uncertainty that characterizes hybrid warfare, the numbers of branches and sequels could be very high, which will put pressure on intelligence and information sources to confirm or deny the indicators.

Key question and actions

- Are the COAs flexible enough to adapt quickly to an adversary’s changes?
- Are the signposts realistic and sufficient to be able to see changes in the COA of the adversary and enable decisions to be taken in a timely manner?
- Have measures of effectiveness been established to see the effects of our actions on the adversary, neutral and friendly actors?
- Is there a constant assessment of the results of our COA regarding the objectives at each time and phase of the operation?
- Are the requests for information and commander’s critical information requirements from higher headquarters and subordinate units available to confirm or discard any

branches and sequels, as well as inform the future operating environment?

The planning process: Step 4 – courses of action analysis

Courses of action analysis – wargaming

4.34. **Rationale and considerations.** The war game must include/account for all the actors with influence in the AOO, it must be used both to confirm the strategy employed by the adversary and, if necessary, revisit the decisive conditions, actions and effects. Wargaming should also identify the need to plan branches and sequels and define the decisive points that will trigger decisions by a commander.

Key questions and actions

- After wargaming our own COA against that of the adversary, can we tell if our COA is flexible enough to adapt to the hybrid adversary?
- After this war game, have enough indicators been identified to confirm or discard the adversary's COA?
- Does our own COA allow us to seize the initiative in non-physical dimension and domains, such as in the cognitive, cyber and information ones?
- Do we have involvement from all stakeholders in the war game?

The planning process: Step 5 – courses of action validation and comparison

4.35. No additional planning considerations from the conventional to the hybrid warfare environment.

The planning process: Step 6 – commander’s course of action decision

4.36. **Rationale and considerations.** When presenting information to the commander, the staff must ensure their logic is presented so that the commander fully understands why particular decisions have, or have not, been recommended. Central to all of this is the commander’s own knowledge, including an understanding and acceptance of the hybrid warfare environment and all that it entails. If the commander does not accept the potential impact that hybrid warfare could have on plans or operations, then all the outputs at this stage will, potentially, be skewed away from where the main threats lie. However, if a commander accepts the potential impact of adversarial hybrid activities on plans and operations, then this will be woven into the outputs of the COA decision process. When outputs are agreed by the commander, it is important for the staff to ensure that the language used recognizes that there is no common, agreed lexicon for hybrid warfare. Therefore, inconsistent use of hybrid warfare-related language can cause confusion with allies and partners when developing plans and can impact relations.

4.37. In the commander's COA decision meeting there should also be present, at a prominent level, representatives for the other instruments of powers and other actors to help shape this decision. This is not to say that the decision must be a collegiate decision, but ideally will be influenced by other important actors to ensure buy in.

Key questions and actions

- What is the commander's level of understanding of hybrid warfare?
- Are unorthodox COA solutions fully thought through and clearly explained?
- Ensure that any outputs have hybrid warfare considerations in them.
- Ensure that any language used is understood by allies and partners.

The planning process: Step 7 – plan development

4.38. **Rationale and considerations.** The development of the plan is a key stage where more hybrid warfare factors and critical dependencies that are vulnerable to exploitation by an adversary will almost certainly be uncovered in the detail, particularly if an adversary changes their strategy. What is critical at this stage is that the right type of working culture has been established where concerns can be raised at any stage – not doing so could be disastrous. In any termination and transition planning it is important to ensure that those focused on helping the re-commissioning of key capabilities for the resumption of normal life for an adversary's population are included to help identify non-military concerns that might impact a seamless transfer of responsibility.

4.39. Any outputs from the headquarters to subordinate formations need to inform them of the hybrid warfare actors present and the possible tactics that may be employed, for example, an adversary may mobilize sections of a local population to blockade key terrain such as bridges to prevent the onward movement of friendly forces. Outputs should also highlight any of the adversary's weaknesses that could be exploited and how that might be achieved without taking the initiative from the local commander. Friendly force vulnerabilities that might need protecting should be highlighted along with suggestions on how this might be best achieved.[69] Subordinate formations may lack expertise in hybrid warfare and tactical actions can have strategic consequences. Therefore, providing as much assistance as possible may be beneficial to coordinating the force.

[69] PMESII analysis would be a good starting point.

Key questions and actions

- Has anything changed?
- Is there the ability to introduce new considerations?
- Has the right working culture been established to allow people to speak up?
- Consider everything that is required to enable the plan. An adversary will seek the softest target that will have greatest impact.
- There is no ‘rear area’.
- Have all possible vulnerabilities been considered in the logistics plan?
- Think innovatively about what constitutes joint fires.
- What role does civil-military cooperation (CIMIC) have in the hybrid warfare environment? Is it now a key enabler?

The planning process: Step 8 – assessment and review

4.40. **Rationale and considerations.** Due to the dynamic nature of hybrid warfare, an adversary will be constantly reviewing their options and changing their plans. They will also be aware of your activities and will seek to cause as much disruption to them as possible at an optimal moment, using all possible instruments of power, including military force. There will be key moments when the plan will be vulnerable to hybrid warfare. These points must be identified and protected as much as possible and this must be kept under constant review.

Key questions and actions

- Is the environment continuously monitored for changes and are they then considered against what these mean for the plan?
- Are key vulnerabilities in the plan understood and mitigated?
- Are identified vulnerabilities still valid as circumstances change?
- If advanced plans have been developed, are they routinely reviewed to see what has changed?
- Be prepared to conduct major changes to the plan as circumstances change.

Chapter 5 – Preparing for tomorrow to reduce the impact

5.1. The complex hybrid warfare environment is here to stay. Major powers will not want to engage in open warfare if they can achieve their aims in a less destructive and disruptive way. Consequently, societies will continue to face threats and challenges from multiple directions, from both state and non-state actors, often simultaneously across physical and non-physical domains. To gain advantage, competitors will continue to target societies' internal and external unity and cohesion with others and their evolving vulnerabilities.

5.2. Additionally, acceleration of scientific and technological advancement, ubiquity and access to dual-use systems, emergence of powerful multinational corporations, private security companies and non-governmental movements are eroding states' monopoly over strategic effects. At the same time, societies face other challenges that can overstretch or draw resources away from the military instrument. They are facing risks associated with climate change, mass migration, transnational organized crime and a shortage of vital resources. All these developments pose increasing risk, causing conflict in one form or another.

5.3. Societies cannot succeed in tomorrow's fight with yesterday's approach. They must prepare for tomorrow's fight today. The battlespace is widening. The line separating war from peace is increasingly blurred by the rising importance of geographically unbound space, cyber domains and a pervasive information environment. A global battlespace will feature more and more diverse state and non-state actors, wielding multiple instruments across all domains and instruments of power to create dilemmas for societies and exploit vulnerabilities.

5.4. Tomorrow's fight will be characterized by persistent strategic competition for advantage influenced by social, economic, demographic, scientific and technological developments. The traditional approach and advantage in defence and deterrence will be challenged by the growing parity of competitors, with tools and methods such as anti-access area denial (A2AD) being shared to create dilemmas. Nuclear weapons will continue to play an essential role in deterring armed aggression but will not deter competition for advantage. Competitors will seek to build advantage using diverse, non-kinetic and kinetic means, across operational domains and civil society. Their actions will significantly complicate the collective ability to recognize the source and nature of the threat or attack, attribute it, and deter or counter it effectively.

5.5. Competition will be persistent and increasingly non-linear. Multiple actors will vie to shape the operating environment to their own strengths, contesting and undermining their adversaries by all means possible. There are known competitors and emerging, powerful new actors who are not controlled by any national government. Competitors are already shaping the widening battlespace of the future to their advantage and contesting the ability of others to achieve military-strategic objectives. They continue chipping away at vulnerabilities in the societies' military instrument of power (MIoP), including influencing open societies and distracting key aspects of civil and military power.

5.6. Societies' MIoP will continue to face prospects of malign, short-of-war actions that may rapidly escalate to short wars as adversaries seek to establish a fait accompli. This means that there are likely to be long campaigns of relative low intensity to manage crisis or support the fight against terrorism. However, near-peer, state actor competitors are pursuing ambitious military modernization programmes and investing in highly disruptive technologies such as hypersonics, robotics, artificial intelligence (AI) and quantum. States and non-state groups or organizations may end up facing global A2AD stalemates, with transparent oceans, exposed communication systems, and critical infrastructure and capabilities held at risk by dual-use, high-velocity, long-range missile systems. All of this is likely to occur against the backdrop of other security challenges, including climate change and pandemics and mass migration, amongst others; these will place an increasing strain on the MIoP.

5.7. Emerging disruptive technologies (EDT) can reinforce existing hybrid threats, while technological developments could present new hybrid threat vectors. In a hybrid scenario, employment of EDTs would enhance most threats. The EDTs assessed as having the most critical impact are 5G, data, AI, autonomy, biotechnology and space, with the potential for quantum technology to further enhance their impacts.

5.8. The mainstreaming of EDTs will create new ethical, legal and moral issues. Societies' civilian and military decision-makers need to explicitly determine EDT employment in countering hybrid threats while remaining within the boundaries and democratic values most societies are built upon. This should include an assessment of where existing training, tactics, techniques and procedures to allow for the effective and ethical use of AI-enabled systems and capabilities. Most importantly, defence officials need a comprehensive view of AI-related initiatives across departments, agencies and international organizations. This is necessary to better anticipate the effects of fielding different AI-enabled systems and capabilities with a view to tactical, operational and strategic objectives.

5.9. The MIoP's ability to sustain a long campaign beyond 'day zero' necessitates reconstruction of resilience along three mutually reinforcing layers.

- Military resilience – those ready forces and capabilities and redundancy that the MIoP requires to ensure its ability to absorb shocks, provide for early resistance and fight through.

- Military-civilian resilience – those plans, processes and connections that must be in place to ensure that civilian support and infrastructure, transport and logistic supplies are a strength rather than vulnerability.
- Civilian resilience – the civil ability to deny competitors the ability to unlock civil vulnerabilities and thereby minimize distraction/overstretch of the MIoP, as well as necessary military support to shield society from malign activities of competitors. This also includes those forces and capabilities that MIoP will be expected to deploy in support of civilian society in the case of natural or human-made disasters.

5.10. Changes in technology need to be considered. For example, Europe and the West is increasingly driving towards a carbon-free economy, which includes fuel. However, other parts of the world, where conflict is more likely, are still heavily dependent on carbon economies. This presents modern armed forces with a dilemma of what to do; if their fuel requirements and other requirements cannot be met by the host nation or are incompatible with their environmental policies then problems may be exacerbated. Equally, this presents numerous opportunities for an adversary to exploit.

What next?

5.11. It is clear that hybrid warfare will form a major part of competition and conflict in the coming years. It has already been adopted by other nations, some in response to what they see as hybrid warfare being conducted against them. To succeed in hybrid warfare, it is necessary to have ‘hybrid’ teams to present ‘hybrid’ solutions. Whilst there is a need people who can warfight there is a growing requirement for people who can understand and are comfortable with operating in the complex hybrid warfare ‘space’. This will require a different way of working, organizing teams, understanding, thinking and problem solving. It will not be a revolutionary moment, it will be evolutionary informed by constant analysis, understanding, experimentation, challenge and listening at all levels.

Lexicon

Part 1 – Acronyms and abbreviations

A2AD - anti-access and area denial

AOI - area of interest

AOO - area of operations

ASCOPE – areas, structures, capabilities, organisations, people and events

CIMIC - civil-military cooperation

COA – course of action

COG - centre of gravity

CHW – countering hybrid warfare

CPOE – comprehensive preparation of the operating environment

EDT - emerging disruptive technologies

IPG - initial planning guidance

IT – information technology

JCOP – joint common operational picture

JIPOE - joint intelligence preparation of the operating environment

LOO - line of operation

MCDC – multinational capability development campaign

MIOP - military instrument of power

MPECI – military, political, economic, civil and information

NTM - notice to move

OLRT - operational liaison and reconnaissance team

PMESII (PT) - political, military, economic, social, informational and infrastructure (physical terrain)

RBIO – rules based international order

SCAEF – stratcom actions and effects framework

TOPFAS – tools for operations planning functional area service

TTP - techniques and procedures

Part 2 – Terms and definitions

Decision-action cycle is the continuous process of deciding what to do based on available information and then implementing actions based on those decisions.

Emic perspective is the ability to view a situation from the point of view of an adversary, may reveal insights that might otherwise have been dismissed.

Etic perspective is viewing a culture or society from your own perspective.

Gradualism are small incremental actions taken by an actor to slowly achieve their aims. Individual actions are rarely significant on their own but all add up to a larger effect.

Horizontal escalation is the applied combination of multiple military, political, economic, civil and informational means, in dynamic degrees of intensity to achieve an effect.

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

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

Measured revisionism are attempts by actors to change an existing order in a small way in their favour.

Non-linearity refers to the unanticipated effects of hybrid warfare attacks that are not usually 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.

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

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

Vertical escalation is the intensified use of one specific means.

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

Whole of government is a co-ordinated, cross-government effort to anticipate, prepare for, respond to or limit the effects of hybrid warfare in the most effective way.

Whole of society broadens whole of government to include other aspects of a society that may prove important in limiting the impact of a hybrid warfare attack.

MCDC

Multinational Capability Development Campaign

For more information, please contact the MCDC Secretariat

MCDC_Secretariat@APAN.ORG