National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Shifting the Mindset Towards Phase Zero: Shaping in the Information Environment

Major Christopher M.F. Ward

JCSP 50

Master of Defence Studies

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 50

Maîtrise en études de la défense

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 50 - PCEMI n° 50
2023 - 2024

Master of Defence Studies – Maîtrise en études de la défense

Shifting the Mindset Towards Phase Zero: Shaping in the Information Environment

Major Christopher M.F. Ward

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

The information environment (IE) represents the battleground of today and tomorrow thanks to advancements in technology, the speed of communications, and the collective power and influence that audiences have on governments and populations. A reactive vice proactive posture to threats, and an inclination to rely on kinetic, physical, and hard-power approaches to dealing with those threats have resulted in a worrying blind spot towards how adversaries are generating effects here at home. Creativity and the power of information are quickly outpacing the exquisite military capabilities Western nations possess to engage in competition and conflict. This hesitancy to engage in the information environment has resulted in a paradox where it appears easier to drop a bomb than to send a tweet. Failure to understand, appreciate, and actively compete in the information environment is not just a missed opportunity, but a critical vulnerability to our sovereignty and national security. A shift in mindset is required consider the effects of our actions in phase zero, before a crisis or conflict has commenced, and to plan and operate in this phase on a persistent basis to shape those environments for our benefit. This paper looks at the existing paradigms regarding warfare, power, and influence and proposes approaches, tools, and methodologies that the CAF and Canada should adopt to be a more active and effective participant in the IE.

SHIFTING THE MINDSET TOWARDS PHASE ZERO SHAPING IN THE INFORMATION ENVIRONMENT

CHAPTER 1 - INTRODUCTION

The exponential advancements in technology over the last thirty years have led to a revolution in how information is generated, shared, and consumed by audiences. The information environment has become a central battleground for below-threshold (of war) activities. Social media has only further accelerated the creation of content and how individuals can influence, shape and manipulate audiences to change behaviours, attitudes, and perceptions. While these methods in a marketing or advertising approach may be more socially acceptable, adversarial governments, militaries, and non-state actors have begun exploiting these tools and techniques to promote their narratives, reinvigorate great power competition, challenge the rules-based international order, and project power using non-conventional means to achieve their end-states.

Recent examples of election interference, foreign influence, and mis-dis-mal (MDM) information campaigns paint a worrying picture of the ways malign actors can generate effects on our home soil, without tripping the conventional indicators for offensive action that could trigger an escalation towards conflict. Canada (and Western governments) are only beginning to recognize the vulnerabilities in their institutions and populations and are struggling to not only identify the sources and vectors of attack, but how to compete and push back against these activities. Prior to this realization, conflict was viewed by the West as a binary between peace and war, whereas our primary adversaries have conformed to a scalable and persistent state of conflict. While peacetime has allowed Western militaries and governments to focus elsewhere, our adversaries have continued to probe our defences, and sought ways to influence or shape environments to their benefit.

To address these new hybrid and below-threshold activities, Canada must move quickly to understand the information environment (IE), the audience and systems analyses that will be required to identify critical vulnerabilities, the targeting enterprises that will facilitate the necessary authorities, the information-related capabilities (IRCs) that will generate effects, and the tools to assess the effectiveness of those initiatives. This needs to be an enduring effort that occurs throughout the continuum of competition, and specifically in phase zero (before crisis or conflict has commenced). Phase zero presents an attractive opportunity to actively shape the environments Canada can expect to operate in and create the conditions to make our intervention and actions more permissive and less contested. Ignoring the potential of phase zero shaping in the information environment represents a crucial opportunity to achieve strategic end-states utilizing smart power initiatives, without automatically resorting to kinetic or lethal means. The level of analysis and rigor required to participate in this arena necessitates a significant commitment of staff, time, and ongoing attention in order to maintain the persistent presence required to remain relevant in the IE.

This paper will seek to explain the existing structures, frameworks, doctrine, and policies that define the information environment; the definitions and key concepts related to communications and narratives; the analytical tools to understand target systems and audiences; and identify the tactics, techniques, and procedures that Canada will need to adapt and adopt to

achieve enduring effects in the IE. All elements described in this paper play a critical role in shaping the information environment during cooperation, competition, confrontation and conflict. It is therefore imperative that Canada not only understand the elements of the IE, but be an active participant and persistent presence during phase zero and throughout the continuum of competition.

CHAPTER 2 – EXISTING PARADIGMS

What comprises warfare, conflict, competition, and cooperation in today's context requires an understanding of the key elements that influence a government's decision-making apparatus. Globalization and the re-emergence of great power competition have highlighted the complexity of state-to-state interaction, the role of non-state actors in influencing national policy, and new complexities around hybrid war and below-threshold activities. No longer can the military be expected to project power and influence alone around the world, and must rely on a whole-of-government (WoG) approach to achieve strategic aims. This chapter will discuss these areas, and their role in guiding decision-making for information operations during, but also pre-conflict in phase zero.

The DIME Construct

The instruments of national power (Diplomatic, Informational, Military, and Economic) represent the primary levers that governments can use to pursue national objectives. Not to be used in a siloed fashion, these instruments are to be employed as complementary and supporting of each other in order to generate effects by influencing other states and actors. The elements are described in greater detail below.

The diplomatic arm incorporates embassies/ambassadors, treaties, policy, and negotiation to achieve effects through outreach and diplomacy. Global Affairs Canada is the primary organization for developing diplomatic initiatives which may seek support from allies and partners to form coalitions or alliances. They may also seek to negotiate with competitors or adversaries to reach agreements or settle disputes.

The military component of national power should be the most familiar, as it may be the most visible and imposing of the four and contains the operations, power projection, deterrence, and is of significant size (both in terms of personnel and equipment). A military can be deployed to conduct any number of activities both to implement or maintain peace, or act as a presence to deter other groups from acting in a certain way. The Department of National Defence in Canada is charged with enabling the 'M' in DIME and is mainly used in an overt and highly visible manner as a hard power resource.

Economic tools can also be leveraged to influence individuals, audiences, or other states. Trade policies, fiscal or monetary policies, sanctions, tariffs, or embargos are all tools that can be deployed to generate an effect or behavioural change.

The informational instrument of power may be the least understood, but its importance has increased exponentially in recent years. Western militaries hard power initiatives have forced adversaries to adopt operations in the information environment to counter this physical dominance using soft power and below the threshold (of war) activities. All government departments influence the information environment. Actions in the information domain include military information support operations (MISO)/PSYOPS, public affairs, and strategic communications.

Any action that the GC takes should consider the combination of these four instruments to maximize the national strategic effect it wishes to achieve, by the most economical means.

Too often has one instrument been employed, without the support or reinforcement of other effects. As with other layered approaches that will be discussed within this paper, synchronization, integration, and alignment of strategic objectives with the activities the government conducts, will become increasingly important.

The Continuum of Competition

Western countries have typically viewed the interaction between countries on a scale from peace to total war. Therefore, there is a need to rethink this model as a continuum of competition that can be used to better inform the state of relations or strategy between nations. This continuum moves from cooperation, rivalry, confrontation, to armed conflict; with an element of competition as one approaches armed conflict as shown in figure 2.1. The US views a similar competition continuum that includes cooperation, competition, and conflict[1]. Ultimately, every nation should expect to be in some persistent state of strategic competition with another along this continuum.

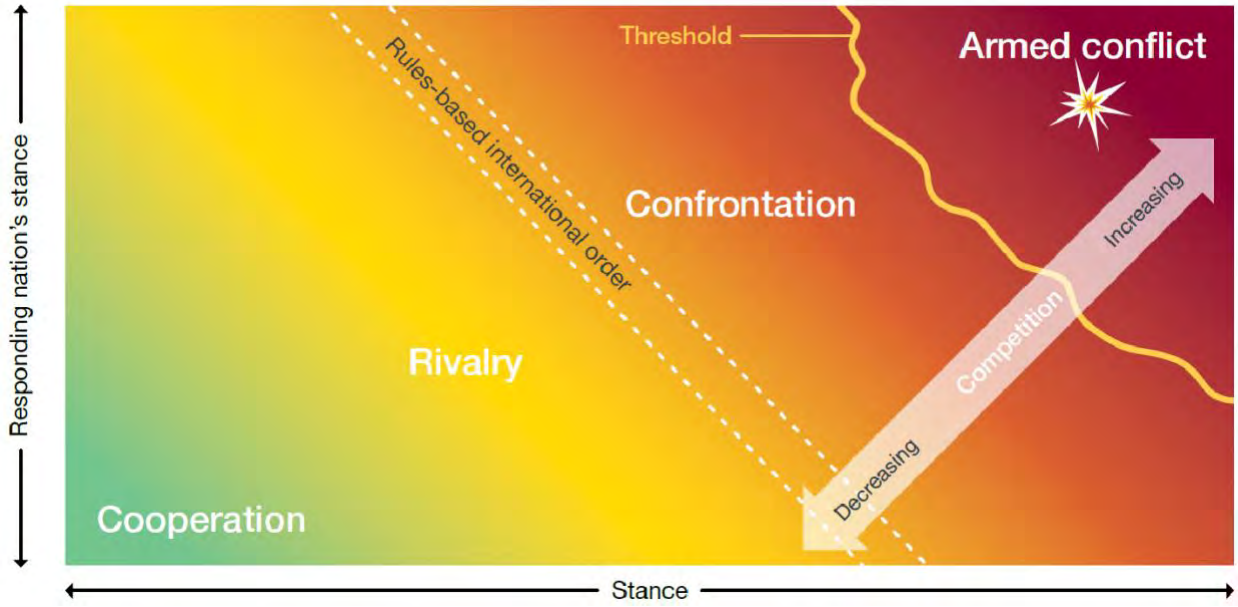


Figure 2.1: The Continuum of Competition

Source: UK Ministry of Defence, 'Allied Joint Doctrine for Information Operations'. 5

Cooperation includes things like engagement and maintaining or advancing relationships in support of policy objectives. Themes within competition include managing strategic or military advantages, enhancing a nation's position over another, or delaying a competitor from

[1] US Joint Force Development, 'Competition Continuum', Doctrine Note (US Joint Chiefs of Staff, 3 June 2019). 2-3

achieving their aims. Lastly, armed conflict relies on defeating, denying, degrading, or disrupting another in a more conventional and military manner[2].

Recognizing that all interactions, even between friendly nations fall somewhere on this spectrum, and is important to informing how to communicate with one another, what types of effects could be achieved, and how to escalate or de-escalate a situation. The binary between peace and war is no longer relevant to the 21st century global environment, where the rules-based international order is increasingly under threat, and the resurgence of great power competition threatens the institutions (such as NATO) that have benefited the West since the end of the Cold War. Canada must position itself to cooperate and compete on a persistent basis and confront or engage in conflict when required. Assuming that the absence of war means we are at peace is no longer a valid assumption.

Types of Power

Power can be defined as "the capacity to do things, but more specifically…the ability to affect others to get the outcomes one wants"[3]. Within the concept of power, hard and soft power at the nation-state level have been deployed to achieve strategic aims. While hard power has dominated the global and grand-strategy space for millennia, the rise of soft power has offered a less violent or overtly destructive alternative for countries to compete and negotiate resolutions to mutual issues. The re-emergence of great power competition, the rapid evolution of technology, and the importance of information have led to the creation of the hybrid term *smart power*.

If power is the ability to influence others to act in ways that one would not have acted otherwise, then hard power is the ability to coerce them to do so[4]. The military has been the primary domain for the projection of hard power, although economic sanctions and coercive diplomacy can also be employed to achieve strategic ends[5]. The "Shock and Awe" campaign to initiate the 2003 invasion of Iraq is a recent example of this.

Soft power relies on persuasion vice coercion. Depending on the situation, this method can be equally or even more effective than hard power, but because it lacks the visible or tangible punch that hard power offers, it usually finds itself in a subordinate position. The difficulty with utilizing soft power lies in the perception of the name itself. Senior leaders and politicians face an uphill battle trying to convey strength or power without suggesting coercive means. Soft solutions simply aren't as convincing or appealing due to their lack of tangibility or visible impact. Hollywood as an exporter of American culture and values to a global audience could be seen as a soft power initiative.

Smart power then, is "the capacity of an actor to combine elements of hard power and soft power in ways that are mutually reinforcing such that the actor's purposes are advanced

---

[2] US Joint Force Development. 5-6

[3] Joseph S. Nye, 'Soft Power: The Evolution of a Concept', *Journal of Political Power* 14, no. 1 (2 January 2021): 196–208, https://doi.org/10.1080/2158379X.2021.1879572. 197

[4] Ernest J. Wilson, 'Hard Power, Soft Power, Smart Power', *The ANNALS of the American Academy of Political and Social Science* 616, no. 1 (1 March 2008): 110–24, https://doi.org/10.1177/0002716207312618. 114

[5] Wilson. 114

effectively and efficiently"[6]. Promoting the concept of smart power relies on the ability to demonstrate soft power approaches using hard power language. Wilson also provides a list of considerations for the employment of smart power[7]:

- The *target* over which one seeks to exercise power—its internal nature and its broader global context. Power cannot be smart if those who wield it are ignorant of these attributes of the target populations and regions;
- *Self-knowledge* and understanding of one's own goals and capacities. Smart power requires the wielder to know what his or her country or community seeks, as well as its will and capacity to achieve its goals;
- The broader *regional and global context* within which the action will be conducted; and
- The *tools* to be employed, as well as how and when to deploy them individually and in combination.

Smart power can be summarized as the surgical dissection of a problem through the use of the right tool (or combination of tools) at the right time to achieve an end-state. The ability to employ smart power requires anticipation, understanding, and creativity to address problems early. Hard power is usually the last resort, but due to a lack of foresight or prudent contingency planning, quickly becomes the first choice when a response is required. The success of smart (and even soft) power relies on the ability to articulate the advantages of these approaches compared to their hard power counterparts. The ease and reliance on hard power to achieve strategic ends ignores the more effective or efficient tools to achieve the same results at a fraction of the cost. Canada must not only understand how all levers of national power influence a problem, but how to combine and layer these to achieve redundancy and a greater strategic result.

The Evolution of Warfare

> *There is ultimately little value in reinforcing a Maginot line of theory that hybrid actors have already bypassed in practice*.
>
> – Matt Petersen[8]

The characterization and definitions associated with warfare continue to evolve, with limited agreement on what each actually means and represents. Terms like regular, conventional, irregular, hybrid, grey zone, and liminal warfare offer insights into how conflict are being waged on a daily basis, without crossing the traditional lines leading to an official declaration of war.

---

[6] Wilson. 115

[7] Wilson. 115

[8] Matt Petersen, 'Competition and Decision in the Gray Zone: A New National Security Strategy', The Strategy Bridge, 20 April 2021, https://thestrategybridge.org/the-bridge/2021/4/20/competition-and-decision-in-the-gray-zone-a-new-national-security-strategy?format=amp. 5

Regular, traditional, or conventional warfare should be clear to most Western audiences. These are the conflicts where militaries engage other militaries to seize territory and settle diplomatic disputes. These include declarations of war, laws of armed conflict, etc… that clearly define how belligerents will act.

Today's hyper-connected world, and a rise in non-state, proxy or non-attributable actors have led to irregular and hybrid models that do not conform to the traditional tenets of warfare. This form doesn't just seek to destroy an opponent's military, but to target public opinion and influence the political decision-making process[9]. Irregular and hybrid threats are designed to operate below the threshold of armed conflict to create confusion or ambiguity, while normalizing such behaviours so as not to attract an unwanted response. China's actions in the South China Sea represent a projection of power and influence over the region; by creating Chinese territories using man-made islands instead of invading or seizing existing lands. This shift in approach can be summarized with a line from *Unrestricted Warfare: China's Masterplan to Destroy America* which states:

> … the new principles of war are no longer "using armed force to compel the enemy to submit to one's will," but rather are "using all means including armed force or non-armed force, military, and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests[10].

Operations in the information environment, using enablers such as space, cyber, and proxy forces are an incredibly effective tool to achieve effects without tripping the indicators and warnings that the West is looking to react to. By the time the audiences realizes they are in conflict with these types of adversaries, they have already ceded a significant advantage to them.

The West's successes in the two world wars of the 20th Century have hindered their ability to address emerging and evolving styles of warfare employed by adversaries. Hoping for a future peer-on-peer conventional conflict utilizing massed conventional forces, with exquisite capabilities, on a defined battlefield is simply not the case anymore. The "big war" paradigm suggested by Hoffman[11] identifies a massive blind spot for Western nations, who will continue to prepare for a war that our adversaries simply don't have the will or ability to fight.

Until Canada acknowledges the plethora of conflict types being conducted to target its population on a daily basis, while staying below the threshold of traditional warfare, they will remain vulnerable and at great risk to losing the next war.

---

[9] Petersen. 1

[10] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Medina University Press International, 2021). xxi-xxii

[11] Frank G. Hoffman, 'Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges', *Prism : A Journal of the Center for Complex Operations* 7, no. 4 (November 2018): 30–47. 31

Effect Dimensions

The information environment is composed of many actors spanning individuals, organizations, and systems that produce, consume, manipulate, and act based on the informational inputs present. The physical, virtual, and cognitive dimensions makeup the effect dimensions in the information environment, and are interrelated to produce effects by changing perceptions, attitudes, and behaviours. AJP 10.1: Information Operations have defined the three dimensions as follows[12].

> The *cognitive dimension* relates to the consequence on the audiences' perceptions, beliefs, interests, aims, decisions and behaviours. This dimension is shaped by culture and societal influences and it encompasses all forms of interaction (such as informational, economic and political) between them. The cognitive dimension is the decisive dimension to achieve an enduring outcome.
>
> The *physical dimension* relates to the consequence on the audiences, the sub-surface, surface, airspace and space areas where all physical activities take place, and where audiences live, including all physical objects and infrastructure that support them. This dimension is divided into a geographical and a physical layer, within which there are entities that can be engaged.
>
> The *virtual dimension* relates to the consequences of activity on the storage, content and transmission of analogue and digital data. It also includes all supporting communication and information systems and processes.

The dimensions are all interdependent on each other to achieve effects, with the cognitive level being the decisive dimension to achieve enduring outcomes[13]. A strategic communications mindset is required to understand how military activities and information are received and perceived in the cognitive dimension. This mindset suggests that when combat operations are involved, creation of cognitive effects should be the primary consideration, and that will align with the manoeuverist approach[14].

Within the three dimensions, are seven layers defined by NATO[15] that further break-down how information flows through the dimensions and are detailed in figure 2.2. The *cognitive layer* is where information is interpreted and non-observable, and comprises an audience's will, cohesion, perceptions, beliefs, interests, values, aims, decisions, and behaviours. The *social layer* where interactions and the sociocultural environment influence decision-making. The *cyber-persona layer* reflects how individuals engage with online profiles (such as X, Facebook, YouTube channels, influencers). The *logical layer* is the data processing, storage and transmission layer contained within networks that receives, stores and exchanges data and resides almost solely in the cyber domain. The *physical network layer* is the physical

---

[12] UK Ministry of Defence, 'Allied Joint Doctrine for Information Operations', Doctrine (NATO, January 2023). 16-17

[13] UK Ministry of Defence. 16

[14] UK Ministry of Defence, 'Allied Joint Doctrine for Strategic Communications', Doctrine (NATO, March 2023). 22

[15] UK Ministry of Defence, 'Allied Joint Doctrine for Information Operations'. 69-70

transmission structures (masts, antennas, satellites). The *physical layer* are the real-world places where information sharing and communication takes place between audiences. Lastly, the *geographic layer* is how audiences communicate within the limitations of physical geography and climates.

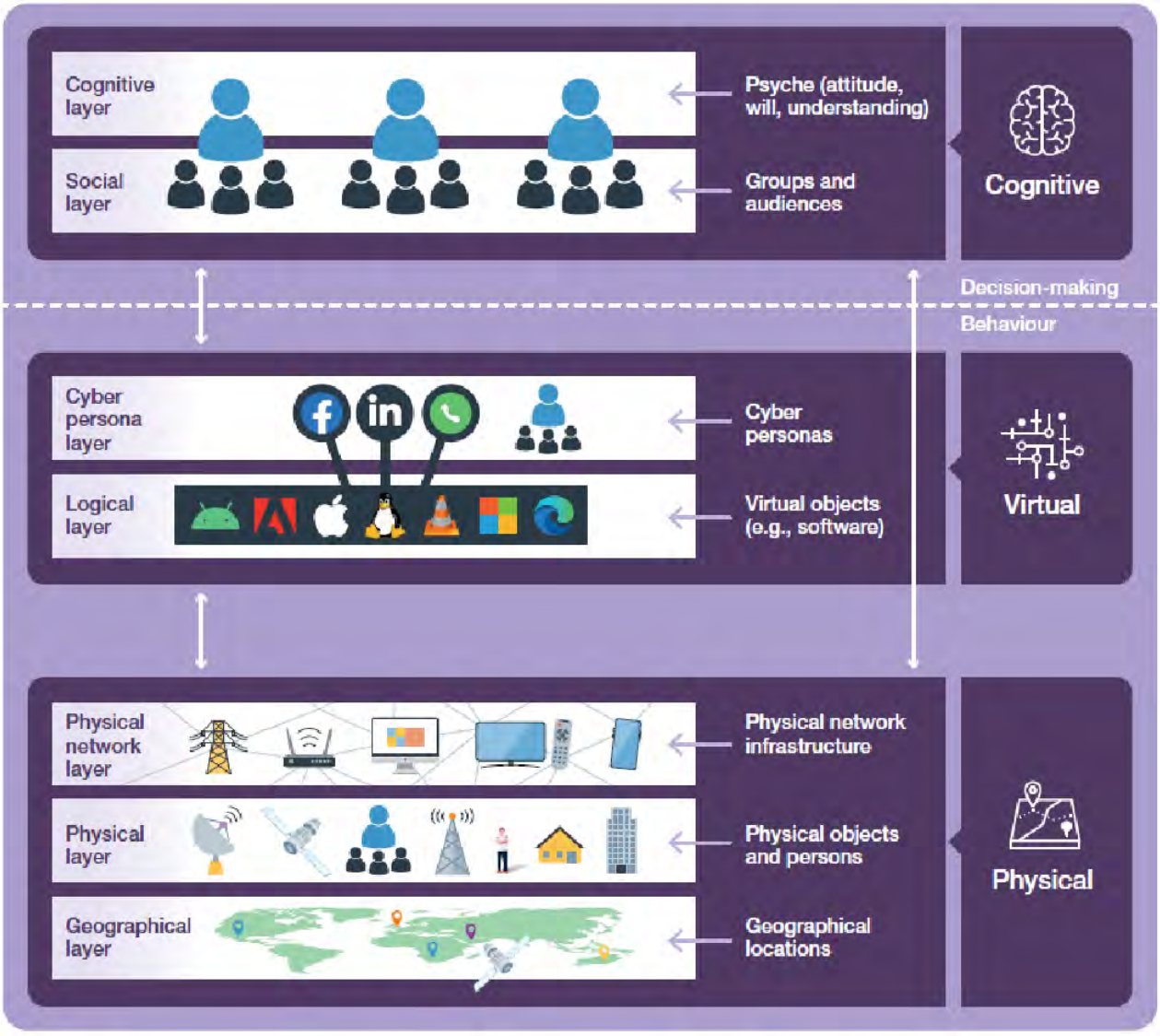


Figure 2.2: The Effects Dimensions and the IE

Source: UK Ministry of Defence, 'Allied Joint Doctrine for Strategic Communications'. 15

Understanding how information and communications flow between transmitters and receivers, and how that information is received and perceived is of critical importance when planning for information operations. Ensuring your message will be received in the way that it is intended, to drive the behavioural change or create the effect desired, requires a greater level of analysis and consideration before undertaking any activity. Conducting this analysis early, and pre-conflict will position planners and operators to quickly deduce the right activities that will send the right message, to the right audience, to deliver the right effects, in the most efficient way possible.

I3O Model – Inform, Influence, and Impose Operations

"I3O" is a model, and communications typology to guide effects and effects generation to address the escalation of information delivery from inform to influence to impose. The means, methods, language, agency, and level of attribution are all tailored to generate one of the three effects within a target audience, and represent a continuum between softer delivery of information, to a more overt and obvious way of messaging a specific group.

Merriam-Webster defines the three effects within I3O as follows. *Inform* is: "to communicate knowledge to; or to impart information or knowledge"[16]. *Influence* is: "the power or capacity of causing an effect in indirect or intangible ways; the act or power of producing an effect without apparent exertion of force or direct exercise of command; to affect or alter by indirect or intangible means; or to have an effect on the condition or development of"[17]. Lastly, *impose* is: "to establish or apply by authority; or to establish or bring about as if by force"[18].

Information-related capabilities (IRCs) can then assume roles within the I3O model based on how they are trying to communicate, the systems they are using to operate in the information environment, and the type of effects they are trying to achieve. The delineation between the three areas resides in the level of agency (the ability to exert free-will or independently choose to effect change) residing in the target audience, and the level of attribution assigned to the originator of the message. Bradley Sylvestre has defined the three areas as follows:

> Inform Operations communicate knowledge of some particular fact and are intended to be conducted under existing conditions in the IE against target audiences with full agency, allowing independent COA selection.
>
> Influence Operations induce, without apparent exertion of force, by targeting conditions in the IE such as narratives, access to information, and amounts of information. Such operations would reduce the agency of a target audience, guiding them towards the selection of a COA that produces a more favourable outcome for friendly forces. Activities undertaken in the IE in support of Influence Operations would likely have attribution mechanisms embedded, enabling activities to be conducted openly, discreetly, covertly, or clandestinely.

---

[16] 'Definition of INFORM', Merriam-Webster, 17 March 2024, https://www.merriam-webster.com/dictionary/inform.

[17] 'Definition of INFLUENCE', Merriam-Webster, 16 March 2024, https://www.merriam-webster.com/dictionary/influence.

[18] 'Definition of IMPOSE', Merriam-Webster, 16 March 2024, https://www.merriam-webster.com/dictionary/impose.

> Impose Operations are applied authoritatively and are orchestrated to remove all agency of the target audience and force capitulation to a narrative beneficial to friendly forces.[19]

When planning operations in the information environment, careful consideration must be given to how messages and information will be delivered and what effect they are designed to achieve. The I3O model therefore should be employed by all information-related capabilities (IRCs) when planning and conducting any operation.

Adversarial Effects (Mis-Dis-Mal-Information)

The terms misinformation, disinformation, and malinformation (MDM) have risen in prominence in recent years as the hyper-connectivity of communications and social media have led to their widespread use to influence the perceptions, attitudes and behaviours of unsuspecting audiences. The confusion over what is real, what the truth is, and what are outright lies have led to a level of skepticism where distrust in government organizations, non-state institutions (schools, churches, etc…), scientific advice and even the news itself is brought into question.

The Communications Security Establishment (CSE) and the Canadian Centre for Cybersecurity have defined MDM as follows. Misinformation "refers to false information that is not intended to cause harm"[20], disinformation "refers to false information that is intended to manipulate, cause damage, or guide people, organizations, and countries in the wrong direction"[21], and malinformation "refers to information that stems from the truth but is often exaggerated in a way that misleads and causes potential harm"[22].

---

[19] Bradley Sylvestre, 'A Typology for Engaging in the Information Environment: Inform, Influence, Impose Operations (I3O)', *On Track: Conference of Defence Associations Institute* 28 (June 2022): 13–18. 17-18

[20] Canadian Centre for Cyber Security, 'How to Identify Misinformation, Disinformation, and Malinformation', Canadian Centre for Cyber Security, 23 February 2022, https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300.

[21] Canadian Centre for Cyber Security.

[22] Canadian Centre for Cyber Security.

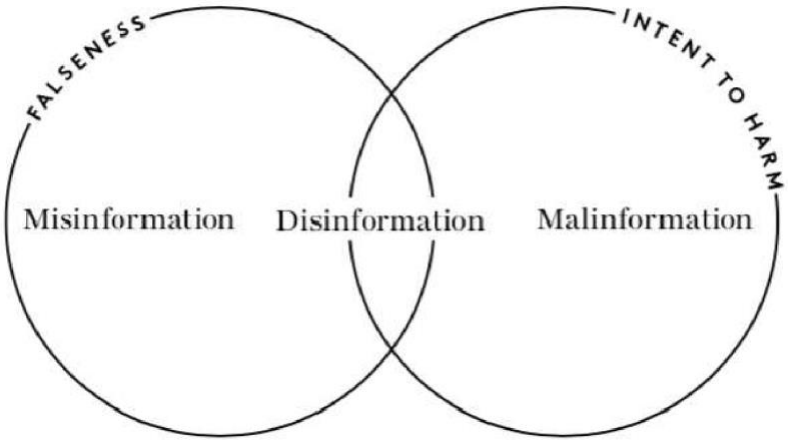


Figure 2.3: Relationship between MDM-Information

Source: Wardle, 'Understanding Information Disorder'. 2

Adversaries employ MDM as part of an overarching narrative, with the goal of stoking social tensions, and amplifying grievances of groups, individuals, or institutions as part of a longer-term process to inflict social, political, and economic divisions[23]. Within these processes, there must reside some instances of truth in order to lend credence to the message or argument they are trying to make. Considering the volume of information that is distributed, and the multitude of vectors and mediums that that information can be received, adversarial narratives can be viewed as mob-like and collective as part of a networked conflict[24]. A networked conflict relies on four main components to be effective. *The source* is the person, group, or organization that that develops the messaging plan. *The domain* represents the communications platform that will be used to disseminate the message. *The message* is based on the narrative, and considers cultural context, language, among other factors and considers the type of media (text, picture, video, etc…) or style (short or long form) that will resonate most. Lastly, *the impact* is the effects on the recipient or audience to include attitude, perception, or behavioural change. A diagram of the networked conflict is included in figure 2.4.

[23] Ben Decker, 'Adversarial Narratives: A New Model for Disinformation' (UK, August 2019), https://www.disinformationindex.org/. 4
[24] Decker. 8

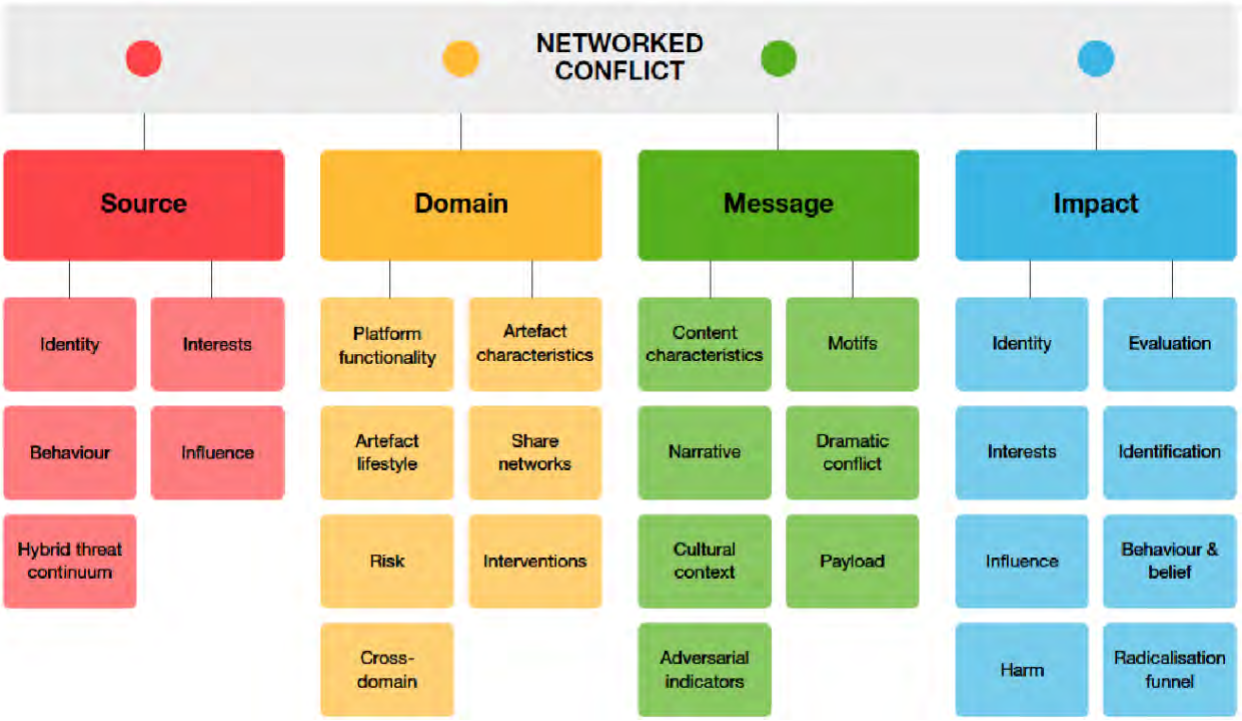


Figure 2.4: Networked Conflict and its Components

Source: Decker, 'Adversarial Narratives: A New Model for Disinformation'. 8

Examples of MDM are prevalent in todays society. Terms like *fake news*, *deepfakes*, *botnets*, *troll farms*, *clickbait*, *alternative facts*, and many more are all ways to influence audiences, re-set the narrative, or revise history to suit a source's aims[25]. One lone instance of MDM is likely not enough to sway an audience's perception, but when combined with multiple methods, over different platforms, and in an engaging, exaggerated, or sensationalized way, it will garner more attention. A scale with examples and severity of MDM is highlighted below in figure 2.5.

[25] Dasha Litvinova, 'How the Kremlin Weaponized Russian History - and Has Used It to Justify the War in Ukraine', CTVNews, 21 February 2024, https://www.ctvnews.ca/world/how-the-kremlin-weaponized-russian-history-and-has-used-it-to-justify-the-war-in-ukraine-1.6777119.

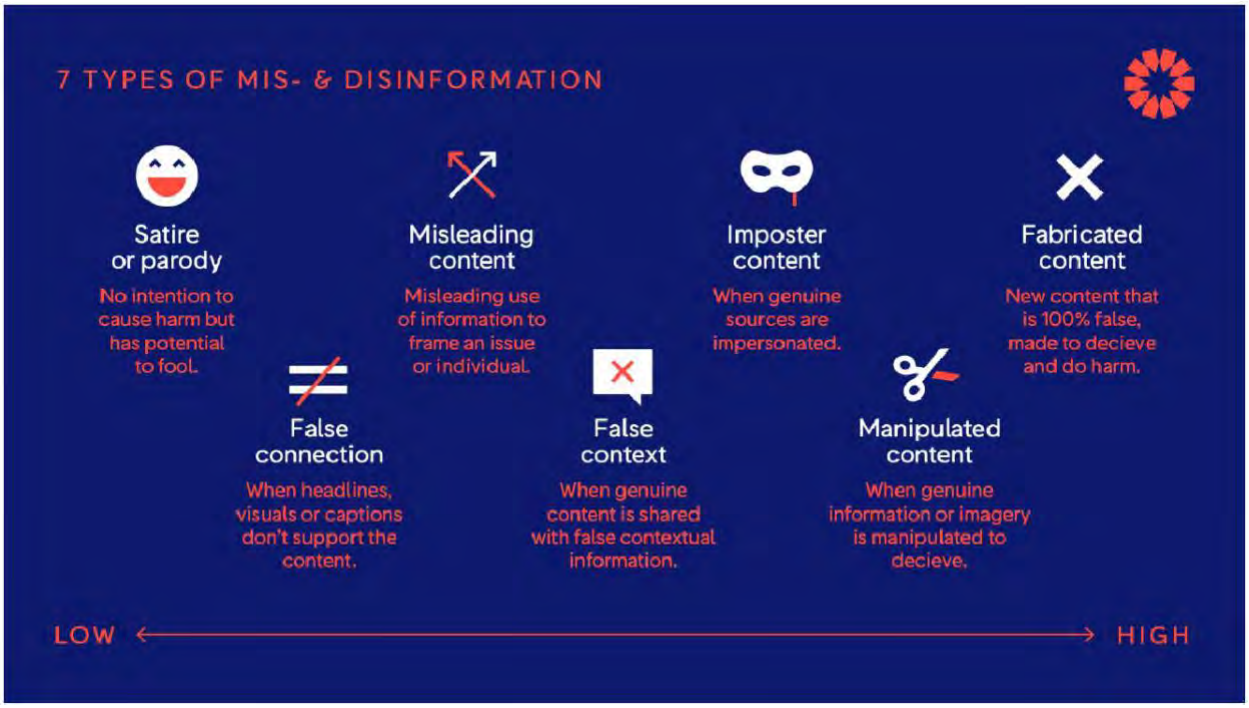


Figure 2.5: Types of Mis- & Disinformation

Source: Wardle, 'Understanding Information Disorder'. 3

MDM will continue to pose challenges to legitimate organizations, institutions, and the truth itself. The use of AI to craft authentic-looking messages, that contain some factual information, and distributed to audiences that are prone to believe the narrative being sold only further complicates the problem. Discerning what is real, from what has been manipulated will rely on the recipient's ability to think critically, consider the source of the information, and compare it against other known facts. Educating the population on what MDM is and how to identify it will be critical ensuring populations are protected, while remaining properly informed.

CHAPTER 3 – THE APPROACH

After discussing the elements that reside within the information environment and how that interfaces with Western approaches to today's competition and conflict, it will be important to look at the ways and means available to Canada to be a persistent and effective presence in the IE. Understanding how to communicate with audiences through words and actions to send the right message to inform, influence, or impose a beahviour or perception change will prove vital in today's hyper-competitive and globalized environment. Strategic communications, narrative-led operations, target systems and audience analyses, distribution of messaging and the ability to incorporate these non-kinetic approaches into routine planning and operational methodologies will be critical to competing with state and non-state adversaries.

Strategic Communication (STRATCOM)

> *The two words 'information' and 'communication' are often used interchangeably, but they signify quite different things. Information is giving out; communication is getting through.*
>
> – Sydney J. Harris[26]

Strategic communication is an activity that recognizes that everything will have a communicative effect to a multitude of audiences. Information, in the form of actions, words, and images that are synchronized and aligned to a compelling narrative will shape the perceptions, attitudes, and behaviours of individuals and groups. Understanding the environment, and defining the audiences that will receive the message, is an important responsibility for planners and communicators. "Audience perceptions are dependent upon the information available to them, so agility and proactive action in the information environment is critical to operational success"[27]. Employment of strategic communications represents a force multiplier when it comes to achieving strategic goals. NATO defines STRATCOM as:

> …the integration of communication capabilities and information staff function with other military activities, in order to understand and shape the information environment, in support of NATO strategic aims and objectives.[28]

Alignment between deeds and words represents a critical vulnerability in effective strategic communications. Activities must be conceived with their communicative effect in mind (what that activity will communicate to each audience), and what perception, attitude, or behaviour it is trying to change. From there, the messaging of those activities must retain a level of consistency so as not to introduce a say-do gap. Consistency and alignment of activities and messages must span from the tactical to strategic levels. The trust and legitimacy of actions depend on minimizing any possible gap between what is said and what is done.

---

[26] UK Ministry of Defence, 'Allied Joint Doctrine for Strategic Communications'. 2

[27] UK Ministry of Defence. 20

[28] UK Ministry of Defence. 3

Effective STRATCOM requires a comprehensive approach that spans all elements of DIME and extends to include allied and partner nations. Three main elements within NATO's approach to STRATCOM include[29]:

- **Understanding** – of the environments, audiences, networks, behavioural drivers, cultures, attitudes, linguistic nuances, and how information is perceived and processed;

- **Integrated Planning** – by using a behaviour-centric approach, while acknowledging how different actions may be received and interpreted by different audiences. This planning also includes consideration for second and third order effects in the cognitive dimension; and

- **Narrative-led Execution** – by deriving and executing activities that are aligned to a central overarching narrative to influence audiences and provide context to the situation.

Principles to guide NATO STRATCOM include values-based, objective-driven, credible, aligned, informed, integrated, empowered, and focussed[30].

Beyond STRATCOM is the concept of Defence STRATCOM employed by the UK and is used to communicate defence activities and is defined as "advancing national interests by using Defence as a means of communication to influence the attitudes, beliefs and behaviours of audiences"[31]. The five principles of this approach are as follows[32]:

- **Strategic military planning must be predicated on appropriate analysis**. An understanding of target audiences and the information environment within which they exist are essential prerequisites of strategic military planning;

- **Strategic military direction must focus on audiences and desired attitudes and behaviours**. Strategic military direction must set out the target audiences whose behaviour the UK government wishes to change or maintain. Success is changing or maintaining behaviours as intended;

- **All Defence assets are a potential means of communication**. Activities should communicate by design using a planned and synchronised combination of actions, images and words. They should employ appropriate Defence assets, whether in their primary role or not;

---

[29] UK Ministry of Defence. 22-23

[30] UK Ministry of Defence. 25

[31] UK Ministry of Defence. 4

[32] UK Ministry of Defence. 26

- **Strategic narratives must be fought for**. Defence's actions, images and words must consistently align with the relevant strategic narrative to build and maintain credibility. Maintaining the initiative will require a proactive and innovative approach. Hard-earned credibility with audiences must be protected; and

- **A continual 'influence cost/benefit analysis' is required**. There will be an ongoing 'influence cost/benefit analysis' to identify the most advantageous, or least disadvantageous, combination of activities. Defence activities that generate influence to the advantage of the UK government within a given target audience may also generate influence to the government's disadvantage in respect of other target audiences.

Phase Zero

Defining what phase zero is, and what it represents in terms of shaping the environments that will be contested today and in the future is critical to the arguments in this paper. "Phase zero encompasses everything that can be done to prevent conflicts from developing in the first place"[33]. The idea of phase zero is not a new concept and has been used to reflect the period of persistent competition that takes place pre-crisis or pre-conflict. The bifurcated Western view that peace is the norm, and war is an aberration needs to adapt, and to realize that other nations and groups do not acknowledge a peacetime state, and that persistent conflict is the norm[34]. This Western view is defined by a few key elements[35]:

- An emphasis on preventing wars rather than shaping environments;

- A view of risk centered around losing wars rather than the possibility of losing the peace; and

- A desire to excel at high-end warfare over confrontations which may fall short of violence.

US Joint Publication 3-0: Joint Operations lists five phases of planning (Deter, Seize Initiative, Dominate, Stabilize, and Enable Civil Authority) in figure 3.1 and has included a shaping phase prior to Phase 1: Deter and following Phase V: Enable Civil Authority[36]. While the recognition of a shaping phase is positive, it only commences when a planning cycle is started. The lead-time required to generate effects in the information, cyber, and space environments is significant compared to conventional or kinetic effects. The window for phase zero described by US JP 3-0 is likely insufficient to generate meaningful engagement with audiences to deliver measurable results. Plans and campaigns need to adopt a persistent

---

[33] Charles F. Wald, 'New Thinking at USEUCOM: The Phase Zero Campaign', *Joint Forces Quarterly* 43, no. 4 (October 2006): 72–75. 73

[34] R Bebber, 'Information War and Rethinking Phase 0', *Journal of Information Warfare* 15, no. 2 (2016): 39–52. 39

[35] Bebber. 42

[36] US Department of Defense, 'US JP 3-0: Joint Operations' (US Department of Defense, 11 August 2011). V-6

approach, where phase zero shaping remains and enduring consideration for all activities and messaging.

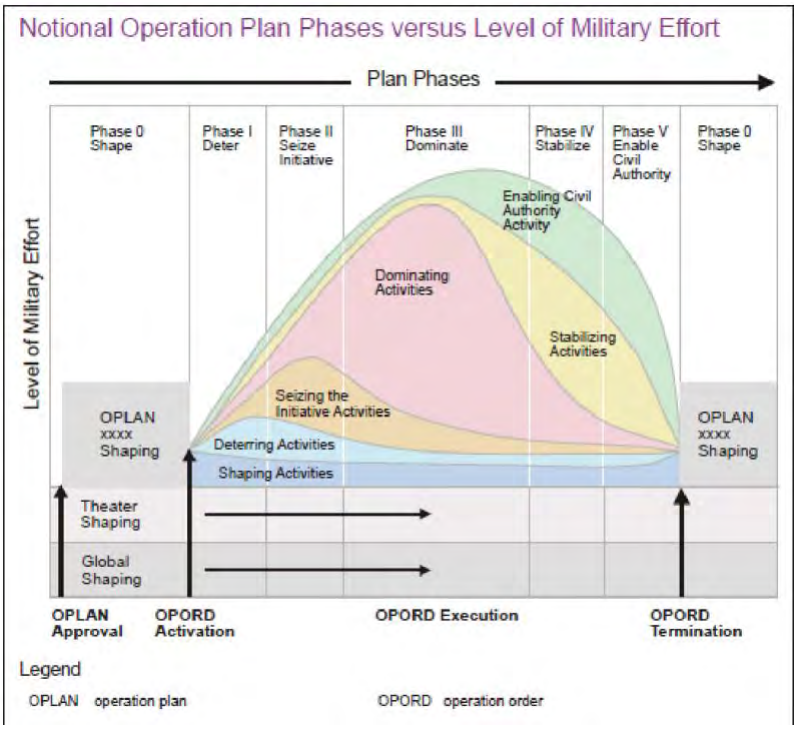


Figure 3.1: Notional Operation Plan Phases versus Level of Military Effort

Source: US Department of Defense, 'US JP 3-0: Joint Operations'. V-6

Russia and China continue to successfully leverage below-threshold activities in phase zero to shape the environment towards achieving strategic objectives. Russia's hybrid war strategy employs information confrontation, destabilizing operations and conventional forces across every domain to challenge and weaken political, military, and economic institutions throughout the world, while seeking to avoid a traditional Western response[37]. China conducts a similar approach based around the concept of *Shi* which aims to use "every possible means to influence the potential inherent in the forces at play" to achieve an optimal competitive position compared to its adversary[38]. When competition escalates into conflict, these nations have already established the upper hand.

The cost and investment required to create effects and achieve success in phase zero is much less than the cost of an exponentially larger conventional conflict[39]. If phase zero is successful, it eliminates the need for the subsequent phases outlined above[40]. Canada must view phase zero (and the associated shaping) as a persistent state of operations, and plan accordingly to compete (and win) before anything escalates towards conflict. The level of planning effort that

[37] Bebber, 'Information War and Rethinking Phase 0'. 44
[38] Bebber. 45-46
[39] Wald, 'New Thinking at USEUCOM: The Phase Zero Campaign'. 73
[40] Wald. 75

is invested to succeed in the "dominate" phase must be applied equally during phase zero, and by utilizing all means available[41]. Success in shaping operations pre-conflict will require a refocus on planning timelines and types of activities but will lead to an optimal position relative to the adversary. Strategies to avoid the war by winning in phase zero should be carefully considered.

Narratives

Narratives play an important role in strategic communications by amalgamating complex ideas, themes, events, and messages into digestible, relatable, and engaging stories for consumption by a target audience. An article by Finlayson and Corman views narratives as a combination of story and discourse, having its own rationality comprising of coherence and fidelity[42]. The story features the basic elements of an event to include the people, actions, adversity, conflict, and the search for an answer, where discourse is the ways and means the narrator conveys and communicates that information[43]. The discussion on coherence and fidelity rests on if the story can follow a logical path and make sense, while fidelity relies on the story's ability to resonate with other stories and experiences we know[44].

NATO defines narrative as "a spoken or written account of events and information arranged in a logical sequence to influence the behaviour of a target audience"[45]. Within this context, there are three types of narratives: institutional, strategic, and micro. The institutional narrative may be stated or generally understood and is the *raison d'être* for that organization. This narrative is the most enduring, although it has the potential to evolve over longer periods of time[46]. The strategic narrative is used to communicate a series of activities that seek strategic outcomes and must align with the institutional narrative[47]. Lastly, micro narratives are aimed at short and mid-term objectives, with alignment of these narratives horizontally across other micro narratives and vertically with the other two higher order narratives being of utmost importance[48].

As mentioned above, alignment within the narrative or set of narratives must be maintained and coherent. The emergence of a say-do gap, where the actions on the ground do not match the messages being sent, creates issues of trust, credibility, and legitimacy with the audiences we are trying to persuade or influence. Some examples of the say-do gap are highlighted below.

Concepts

Employment of narratives in a military context is only just starting to be realized by the West, as recent asymmetric, gray-zone, ideological, insurgent and terrorist-based engagements

---

[41] Bebber, 'Information War and Rethinking Phase 0'. 49

[42] Mark A. Finlayson and Steven R. Corman, 'The Military Interest in Narrative', *Sprache Und Datenverarbeitung (International Journal of Language Data Processing)* 1, no. 2 (2013): 173–91. 174

[43] Finlayson and Corman. 174

[44] Finlayson and Corman. 178

[45] UK Ministry of Defence, 'Allied Joint Doctrine for Strategic Communications'. 28

[46] UK Ministry of Defence. 29

[47] UK Ministry of Defence. 29

[48] UK Ministry of Defence. 29-30

have highlighted the force-multiplying effects of winning the narrative battle. Terms like *operationalizing the narrative* and concepts such as *narrative-led operations* have begun to emerge; requiring a mindset shift among commanders and planners previously consumed by kinetic and capability-based planning.

Narrative-led operations can be defined as "…the purposeful strategic narrative led analysis, planning and execution of operations for the purpose of creating a clear linkage between the strategic intent and the campaign design in order to ensure that the words of the political level are matched by the deeds, images and words of the Joint Force"[49]. This approach identifies the initial steps of the planning process to be the creation of a narrative, or narratives that will dictate the tasks, structures, dispositions, targets, and authorities to a force, and be wholly aligned with the overarching strategic narrative. That narrative will be ingrained throughout the force and considered when guiding all activities, communications, and actions to give meaning and reinforce the narrative.

The ability to craft an effective and engaging narrative rests on the ability to understand language, culture, context, emotion, among other things; and convey it clearly to an identified audience in ways they can comprehend through relevant mediums that they use to consume information. Naturally, not all narratives are created equal, and the quality and traction associated with a narrative will depend on the elements used to create engagement and association. At the most basic level, a narrative should be a collection of details associated with an event or series of events. While accurate and factual, it could lack the engaging qualities that will appeal to the target audience. A narrative that can convey emotion, suspense, tragedy, relatable characters, and captures the audience's imagination will generate a much higher level of retention and promotion. More detail on these specific elements is covered below.

Elements

There are a number of elements from literature and storytelling that can be employed to create or enhance the effectiveness of a narrative. Structures such as PAAIVE (Plot, Archetypes, Associations, Imagery, Values, and Emotions) and Northrop Frye's four literary narrative templates (Comedy, Romance, Irony, and Tragedy)[50] can all be used to frame basic ideas and actions and link them to more engaging, humanistic, and relatable narratives. Effective storytelling using the enhanced techniques described above offers many benefits in the forms of comprehension, memory, thinking, enthusiasm for learning, mastery of languages, and interpretation[51]. Information shared in story-form revealed a level of comprehension and retention that was up to fifty percent higher than other means of conveying the same details[52]. Framing narratives this way, and anchoring it through relatable characters, plot lines, imagery,

---

[49] Thomas Elkjer Nissen, 'Narrative Led Operations', *Militært Tidsskrift (Norwegian Military Journal)* 141, no. 4 (January 2013): 67–77. 75

[50] Suzanne Waldman and Sean Havel, 'Updating the Concept and Execution of Narrative-Led Operations' (International Command and Control Institute, 2021), https://docs.google.com/document/d/1YBuZmVmaykJoiW5Ayo5bFTjhiBfVjIFx/edit?ouid=105032774633316896 85&rtpof=true&sd=true&usp=sharing. 3

[51] Finlayson and Corman, 'The Military Interest in Narrative'. 179

[52] Finlayson and Corman. 178

and emotions allows the audience to connect in a more meaningful way than through basic or robotic language.

Another important component in the narrative space is that of the audience. Who you are speaking to will dictate and shape what your message is, the language and nuance used to convey that message, and the socio, cultural, and economic considerations that must be addressed in transmitting that message. At the highest levels, institutional and strategic narratives must be generic enough to address the array of audiences it will consider, but operational narratives (down to themes and individual messages) can be tailored to specific groups to elicit unique reactions or shape and craft certain behaviours. Who the audience is (internal, external, friendly, adversarial, etc…) and what behaviour or perception you intend to influence will need to be analyzed to inform the narrative development process. Audience analysis will be discussed later in this paper.

Ways

Narrative development should be the first thing to occur when a planning cycle or process is launched. Depending on the level of the planning group, the high-level strategic narratives should be conceived or, at the operational level, will already be made available to drive narrative refinement and determining the effects and activities that need to be undertaken. Once determined, the narrative needs to be operationalized and deployed to the desired audiences. Suzanne Waldman and Sean Havel have proposed the Three Modes of Operationalizing Narrative Effects (figure 3.2) for a narrative to be successful, by relying on storytelling approaches vice highly polished and non-emotive statements. They note that narratives resonate with audiences not because they have been formally presented as such, but through repeatedly encountering stories and actions that testify to the validity of those narratives[53].

[53] Suzanne Waldman and Sean Havel, 'Launching Narrative into the Information Battlefield', *Connections: The Quarterly Journal* 21, no. 2 (2022): 111–22. 115

Figure X: The Three Modes of Operationalizing Narrative Effects

Source: Waldman and Havel, 'Launching Narrative into the Information Battlefield'. 116

The framing of a narrative involves identifying the cognitive parameters and behavioural effects trying to be achieved. Targeted narrative effects are the psychological equivalent to the more conventional mission task verbs used by militaries in the physical dimension. Figure 3.3 demonstrates the relationship between the narrative effects and Frye's narrative templates.

Narrative Template	**Targeted Narrative Effect**
Comedy	REASSURE
Romantic-comedy	INSPIRE
Romance	RALLY
Tragic-romance	FORTIFY
Tragedy	DISRUPT
Tragic-irony	SEVER
Irony	NULLIFICATION
Ironic-comedy	REVERSE

Figure 3.3: Targeted Narrative Effects

Source: Waldman and Havel, 'Updating the Concept and Execution of Narrative-Led Operations'. 4

These elements are then combined with the PAAIVE taxonomy to generate appealing stories and reinforced by actions and activities to increase the resonance and resilience of the narrative.

Examples

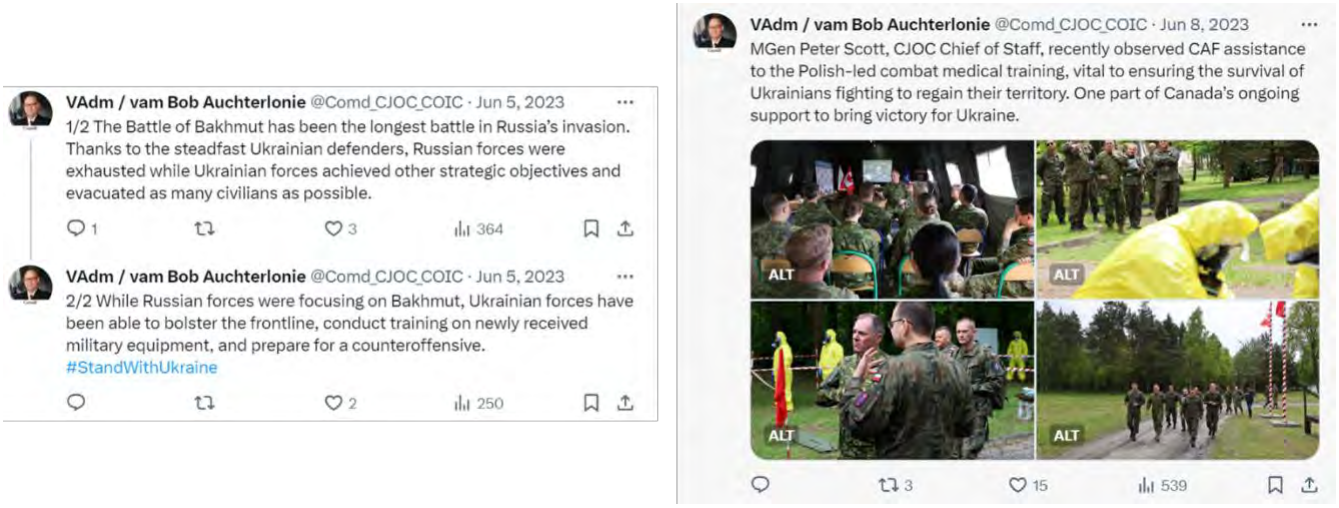


Figure 3.4: PAAIVE Example (Ukraine)

Source: VAdm / vam Bob Auchterlonie s as[@Comd_CJOC_COIC], 5 June 2023.[54]

VAdm / vam Bob Auchterlonie [@Comd_CJOC_COIC], 8 June 2023.[55]

PAAIVE Example – Comd CJOC: The two tweets above from VAdm Auchterlonie (Commander Canadian Joint Operations Command) highlight the struggles, challenges, and successes of Ukrainian forces, Ukrainian populations, and nations contributing to the war effort. Key words like: duration, steadfast defenders, exhausted, achieved, evacuated, bolster, prepare, vital, survival, regain, support, and victory are used to connect with identified audiences and elicit specific responses through messages like this. While a basic narrative would stick to the facts, this example of a more refined narrative seeks to expand on the facts to generate a higher level of engagement.

[54] VAdm / vam Bob Auchterlonie [@Comd_CJOC_COIC], 'The Battle of Bakhmut Has Been the Longest Battle in Russia's Invasion. Thanks to the Steadfast Ukrainian Defenders, Russian Forces Were Exhausted While Ukrainian Forces Achieved Other Strategic Objectives and Evacuated as Many Civilians as Possible.', Tweet, *Twitter*, 5 June 2023, https://twitter.com/Comd_CJOC_COIC/status/1665721414228275200.

[55] VAdm / vam Bob Auchterlonie [@Comd_CJOC_COIC], 'MGen Peter Scott, CJOC Chief of Staff, Recently Observed CAF Assistance to the Polish-Led Combat Medical Training, Vital to Ensuring the Survival of Ukrainians Fighting to Regain Their Territory. One Part of Canada's Ongoing Support to Bring Victory for Ukraine. Https://T.Co/bygKFB4wEY', Tweet, *Twitter*, 8 June 2023, https://twitter.com/Comd_CJOC_COIC/status/1666794825478295555.

Canada deploys CP-140 long-range patrol aircraft to support Haiti

From: National Defence

News release

February 5, 2023 – Ottawa, Ontario – National Defence / Canadian Armed Forces

"Canada is committed to supporting the people of Haiti, as well as peace and security in the country. The deployment of a Canadian patrol aircraft will strengthen efforts to fight criminal acts of violence and to establish the conditions necessary for a peaceful and prosperous future. I thank all members of the Canadian Armed Forces involved in this mission for their service and dedication to global stability."

The Honourable Anita Anand, Minister of National Defence

Canada military plane returns after Haiti surveillance

Published 8:50 PM GMT-5, February 7, 2023 Share

OTTAWA, Ontario (AP) — A Canadian Armed Forces surveillance plane was heading home Tuesday after two intelligence-collecting flights over Haiti.

Figure 3.5: Say-Do Gap Example (CP-140 Deployment to Haiti)

Source: National Defence, 'Canada Deploys CP-140 Long-Range Patrol Aircraft to Support Haiti'.

Associated Press, 'Canada Military Plane Returns after Haiti Surveillance'.

Say-Do Gap: The crisis in Haiti created a demand and opportunity for Canada to respond with military capabilities to provide intelligence, surveillance, and reconnaissance (ISR) to disrupt gang activity, bolster efforts to establish and maintain peace and security, and demonstrate Canada's commitment to the Haitian people[56]. The announcement was made on 5 February 2023, and after 2 ISR flights by a CP-140 Aurora, the aircraft redeployed to Canada two days later on 7 February. Of note, two maritime coastal defence vessels (MCDV) were re-tasked from Op PROJECTION-West Africa for a limited period of three weeks at that same time as well. This news release by the MND and the limited actions in the region raise questions of coherence to the narrative.

[56] National Defence, 'Canada Deploys CP-140 Long-Range Patrol Aircraft to Support Haiti', news releases, Government of Canada, 5 February 2023, https://www.canada.ca/en/department-national-defence/news/2023/02/canada-deploys-cp-140-long-range-patrol-aircraft-to-support-haiti.html.

Figure 3.6: Non-Aligned Example (Diversity)

Source: General / Général Wayne Eyre [@CDS_Canada_CEMD], 11 February 2021.[57]

Non-Aligned: This message features a strong narrative speaking to inclusion, diversity and a commitment among senior leaders to "champion culture change". The photo used however, features a conference room full of middle-aged white males, creating a level of irony between the message and accompanying imagery.

Conclusion

Narratives must always be thought of, formed, and developed in terms of story, discourse, coherence, and fidelity[58]. The importance of the narrative and narrative-led operations cannot be understated when it comes to achieving success across the continuum of competition. A valuable tool within the strategic communications framework, effective storytelling serves as a sensemaking function across all audiences and aims to give meaning and promote understanding of the organization's aims, intents, and end-states. Working in terms of *narratives* and *effects* reveals a multitude of potential courses of action previously constrained by those focussed more

[57] General / Général Wayne Eyre [@CDS_Canada_CEMD], 'Conversations on Diversity, Inclusion, and Culture Change Are Not Incompatible with Our Thirst for Operational Excellence. I Count on My Senior Leaders to Champion Culture Change. Diversity Makes Us Stronger, Inclusion Improves Our Institution. We Are #StrongerTogether - ArtMcD Https://T.Co/y4piRhtW3N', Tweet, *Twitter*, 11 February 2021, https://twitter.com/CDS_Canada_CEMD/status/1359743611349438464.

[58] Finlayson and Corman, 'The Military Interest in Narrative'. 174

on capability-based planning and kinetic effects. Leveraging the multiple domains and smart-power tools to deploy the narrative will yield much greater results than realized in current conflicts.

When properly employed in phase zero and before the commencement of kinetic operations, narratives can be deployed to shape host-nation populations to be more amenable to our cause, solidify support from our domestic audiences, educate our troops about the actions they will be expected to undertake, deter opponents or adversaries from conducting hostile actions against us, and engage a bevy of other audiences to levy effects that could aid in the successful undertaking of operations. It is also important to note that once kinetic actions commence, the need for narrative development and evolution does not cease, and must remain responsive to the situation, leading to timely and iterative change.

Narrative alignment and minimization of the say-do gap will also remain a concern when it comes to trust, authenticity, and legitimacy in the eyes of all internal and external audiences. While winning the narrative battle is an almost impossible endeavour, defeat is virtually inevitable in the absence of constant engagement, communication, and messaging. Prudent planning, analysis, coordination, synchronization, and timely reaction to events will ensure an adaptive narrative that can be tailored to address any number of contingencies.

Personas

The volume and flow of data in today's information environment can easily overwhelm the typical user. To address this, the concept and deployment of personas are used to provide an archetype or profile that represents the traits of a target audience. "Personas are not real people, but they are based on the behaviours and motivations of real people"[59]. Creating effective personas isolate sub-groups and audiences with predictable traits, attitudes, beliefs, and behaviours, which makes communicating and messaging with them much easier. While creating these personas (think social media accounts) is easy, the refinement and engagement required to actually reflect an audience and capture their attention requires more effort.

The development of effective personas can be modelled, but requires considerable analysis to identify target audiences with meaningful patterns in user behaviour in order to turn those into archetypes that represent a broad cross-section of users[60]. The 7-step model for constructing personas are detailed by Cooper et al and is outlined below[61].

- Identify behavioural variables;
- Map interview subjects to behavioural variables;
- Identify significant behaviour patterns;

---

[59] Alan Cooper, Robert Reimann, and David Cronin, *About Face 3: The Essentials of Interaction Design* (Indianapolis, IN: Wiley Publishing, 2007). 75

[60] Cooper, Reimann, and Cronin. 76

[61] Cooper, Reimann, and Cronin. 97

- Synthesize characteristics and relevant goals;
- Check for redundancy and completeness;
- Expand description of attributes and behaviours; and
- Designate persona types.

In practice, especially in today's social media environment, the line between real and fictional personas have been blurred. Social media profiles, influencers, and interest groups are able to utilize real people to assume the traits or behaviours that will resonate with their target audience. Whether it is adopted as a profile or persona, a significant amount of role-playing and imagination may be required[62]. Therefore, the lines between real users and a somewhat fictitious online presence are relevant to Cooper's concept of fictional personas representing real users[63].

In addition to promoting UK defence issues, the UK's Ministry of Defence "X" account[64] shares daily intelligence updates on the War in Ukraine (figure 3.7). The posts feature a common look and feel, regular (daily) updates, and offer behind-the-scenes or "insider" information about the ongoing conflict. This approach focusses on attempting to explain the complexities of military, strategic, and great power competition to regular society in a more digestible manner. The trust and engagement that is developed by that account can then be leveraged as a sense-maker or common voice that can communicate effectively with UK society, and other aligned audiences.

[62] Aaron Humphrey, 'User Personas and Social Media Profiles', *Persona Studies* 3, no. 2 (13 December 2017): 13–20, https://doi.org/10.21153/ps2017vol3no2art708. 18

[63] Humphrey.

[64] UK Ministry of Defence, 'Ministry of Defence (@DefenceHQ)', X (formerly Twitter), 24 April 2024, https://twitter.com/defencehq.

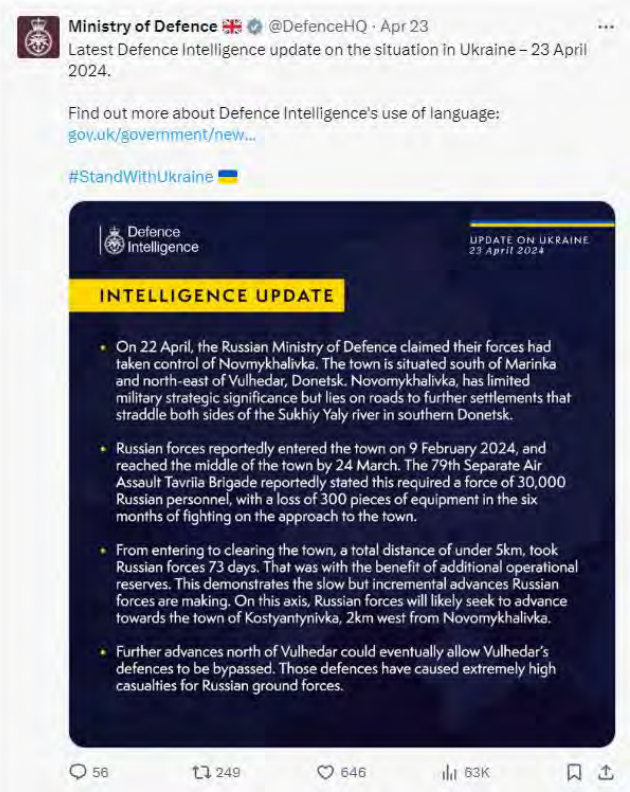


Figure 3.7: UK MoD Intelligence Update 23 April 2024

Source: Ministry of Defence GB [@DefenceHQ][65]

The development of personas to represent important issues for the CAF and GC should continue to be explored, analyzed, and developed as an important means of connecting and communicating with not just Canadian audiences, but allied-global and even adversarial audiences.

Actors

Government departments are ultimately responsible for developing, synchronizing, and coordinating *what* narratives and information are to be shared, while information-related capabilities represent the means and *how* information is deployed. Identifying who the players are in the information environment will lead to a greater understanding of the collective role that everyone plays in communicating with audiences.

---

[65] Ministry of Defence GB [@DefenceHQ], 'Latest Defence Intelligence Update on the Situation in Ukraine – 23 April 2024. Find out More about Defence Intelligence's Use of Language: Https://Gov.Uk/Government/News/Defence-Intelligence-Communicating-Probability #StandWithUkraine UA Https://T.Co/PE81EXaY81', Tweet, *Twitter*, 23 April 2024, https://twitter.com/DefenceHQ/status/1782682068214063215.

Information-Related Capabilities

Information-Related Capabilities (IRCs) represent a number of ways and means to convey or affect the information environment. These tools can be leveraged across the spectrum of cooperation, competition, and conflict to inform, influence, or impose our will on both friendly and adversarial audiences. The intensity and severity of these can be modified and tailored, along with the message and effect they are trying to achieve. These should not be seen as individual silos to achieve affects, but rather a combination of vectors that can be employed simultaneously to broadcast or reinforce messages and information. A brief description of each is provided below.

Public Affairs (PA) may be the most visible example of a communicative element within the CAF. Their primary role is to inform Canadians of military activities taking place at home and abroad in order to demonstrate our role and contributions, while highlighting accomplishments of the organization. While deployed, the public affairs function is able to capture relevant imagery and provide front-line accounts of ongoing operations. They are also primarily responsible for advising commanders regarding communications matters and administering related social media presence and accounts. In order maintain a level of integrity, they are unlikely to directly engage in any influence or impose-type tasks.

Engagement between individuals and organizations can also send important messages to target audiences. This includes everything from strategic engagements between diplomats, key leader engagements (KLE) using the network of defence attachés throughout the world, or even identifying specific areas and locations that the CAF will visit for tactical-level engagements. The size, status, or importance of the meeting or event can be tailored to convey a number of messages to various audiences.

Presence, Posture, Profile (PPP) can be used to send a number of different messages to different audiences and should be carefully considered and curated. Presence is based on where individuals are actually deployed, their capabilities, and size. Posture covers the types of activities that will be undertaken in the area of operations. Lastly, profile focusses on how a force presents themselves to the audience; being in full-fighting order with weapons at the ready will send a different message than soldiers patrolling without helmets or body armour.

Operational Security focusses on the denial of information to an adversary about CAF actions, movements, and dispositions in order to protect and shield the force. Protection of this information is important across all-domains, but none more important than in cyber as digital communications as the use of mobile devices can divulge sensitive details to external audiences (such as US troops exercise routines[66] or Russian-linked Instagram accounts operating in Crimea[67])

---

[66] The Associated Press ·, 'Fitness Devices May Reveal Sensitive Info about Soldiers' Locations | CBC News', CBC, 29 January 2018, https://www.cbc.ca/news/science/fitbit-privacy-1.4508382.

[67] Cullen, 'Russian Soldier Accidentally Gives Away Ukraine Location with Geo-Tagged Instagram Selfies', Independent.ie, 5 August 2014, https://www.independent.ie/entertainment/russian-soldier-accidentally-gives-away-ukraine-location-with-geo-tagged-instagram-selfies/30485060.html.

Civil-Military Cooperation (CIMIC) is an important activity to manage. All deployments have some level of interaction with the local population, who can be an excellent source of intelligence and support for the operation, while offering avenues to promote the friendly narrative. Fostering and nurturing that relationship through positive engagement, cooperation, and promoting mutual benefits can act as a force-multiplier beyond the conventional hard power capabilities and roles present within the military.

Military Deception (MILDEC) seeks to alter or change a perception or behaviour that will influence decision-making processes at the expense of the adversary. It relies on a significant amount of intelligence, analysis, and planning to determine what actions will reinforce their perceptions, or provide enough counter-information to drive them to a different conclusion. Operation MINCEMEAT during WW2 was an example of this[68] and will be expanded upon later in this paper. Information alone will not impose this change, and must be reinforced with realistic and credible supporting actions across the effects dimensions to lead the target to the desired conclusion.

Psychological Operations (PsyOps) are "planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives"[69]. While similar to deception operations, PsyOps has a much greater focus on populations and audiences as opposed to key decision makers.

Space, while a domain unto itself, continues to play a crucial role in enabling pan-domain operations, especially in the information environment. GPS, SATCOM, and other signals utilizing space can be leveraged as a means to distribute information and media, or to send, receive, or monitor communications both friendly and adversarial.

Cyber represents the network of connected systems both wired and wireless that the population uses to create, share, and consume information. The vulnerability of these systems to influence or attack is extremely high due to the speed and ease that data can be shared globally. While offensive cyber operations (OCO) can be employed to destroy, manipulate, or exploit networks and systems, there is an important role for defensive cyber operations (DCO) to defend and protect host-nation systems from external attack.

Electronic Warfare (EW) utilizes the electromagnetic spectrum to conduct attack, defence, or surveillance on an audience or adversary. When used in an offensive role, EW can deny the use of communications, the sharing of information, or can introduce messages onto their systems. Defensive EW seeks to harden and protect our communications from interference or interception by unauthorized elements. Lastly, surveillance and signals intelligence (SIGINT) can be used to intercept and listen-in on communications in order to determine intents and actions from a target audience.

Fires and kinetic activities tend to reside in the physical dimension, but their effects also play a significant role in the psychological domain. The effects generated usually serve a primary

---

[68] Ben Macintyre, *Operation Mincemeat*, 1st ed. (Harmony Books, 2010).

[69] UK Ministry of Defence, 'Allied Joint Doctrine for Information Operations'. 30

function of destroying the targeted entity however, secondary effects in the cognitive dimension can serve to influence behaviours, change perceptions, or achieve a deterring effect against future action by the target audience.

The IRCs discussed above provide a broad idea of what they are and what they can accomplish. They can be used in isolation, or in concert with each other to support or enhance the desired effects to be achieved. Employment of IRCs to date have been relatively siloed or geographically bound to theatres or areas of operation the CAF have deployed to. As we look at the emerging global power competition and the exponential growth of digital communications, it has become increasingly important that all actions undertaken by the CAF be coordinated in order to synchronize actions and to promote the narratives, themes, and messages they want to convey. It is also important to recognize that fires and kinetic action should be utilized only after other forms of inform, influence, and impose have been considered. This will require a level of anticipation and proactive planning in phase zero ahead of the crisis to ensure that other means of influencing the problem can be employed first in hopes of avoiding a more traditional conflict.

Other Government Departments

Other government departments (OGDs) play a crucial role within the national security environment to tackle threats to Canada. The roles and authorities afforded to CAF capabilities and elements cannot cover the range of threats to Canada, nor protect all persons and groups within the population. Therefore, it is imperative that OGDs be leveraged to capitalize on their ability to project capabilities and share information within a comprehensive whole of government (WoG) approach. A non-exhaustive list of Government of Canada (GC) departments that can play an important role in aiding the CAF and government deal with threats to national security is detailed below.

The Royal Canadian Mounted Police (RCMP) is a federal police force. Some of their duties include: law enforcement, investigation of offences, keep Canadians and their interests safe and secure, and assist Canadians in emergency situations and incidents[70]. Additionally, the most recent mandate letter to the RCMP identifies “collaborating with other authorities to combat cybercrimes, money laundering, human trafficking, child sexual exploitation, ideologically-inspired violent extremism, foreign interference and threats to Canada's democratic institutions”[71].

The Canadian Intelligence and Security Service (CSIS) is Canada’s intelligence service and looks primarily at threats including “terrorism, the proliferation of weapons of mass destruction, espionage, foreign interference and cyber-tampering affecting critical infrastructure”[72]. Their output is generated in the form of intelligence reports and products that

---

[70] Royal Canadian Mounted Police, ‘About the RCMP | Royal Canadian Mounted Police’, 31 October 2019, https://www.rcmp-grc.gc.ca/en/about-rcmp.

[71] Royal Canadian Mounted Police, ‘Commissioner’s Mandate Letter’, Royal Canadian Mounted Police, accessed 17 January 2024, http://rcmp.ca/en/corporate-information/commissioners-mandate-letter.

[72] Canadian Security Intelligence Service, ‘CSIS Mandate’, 30 April 2018, https://www.canada.ca/en/security-intelligence-service/corporate/mandate.html.

will be shared with other departments. While its primary role is to monitor and investigate threats, there exists an ability to reduce threats to national security when needed.

The Canadian Coast Guard (CCG) is an operating agency of the department of Fisheries and Oceans and contributes to the national security instrument through ensuring "Canada's sovereignty and security by establishing a strong federal presence in our waters"[73]. The CCG supports the CAF with mobility options (ie. Icebreaking/transportation) to operate in the Arctic.

OGDs such as the Canadian Border Services Agency (CBSA), Transport Canada (TC), Environment and Climate Change Canada (ECCC), and a number of others are examples of organizations play a significant role in promoting national interests and sovereignty while protecting Canadians at home and abroad. These can all be leveraged based on the threat and vector used to counter adversarial actions utilizing the roles, capabilities, and authorities they possess.

While the above departments focus primarily on domestic security, Global Affairs Canada (GAC) should be seen as an umbrella organization that "define, shape and advance Canada's interests and values in a complex environment…lead humanitarian, and peace and security assistance efforts…and contribute to international security and the development of international law"[74]. As a more outward or international-facing organization, it is able to address the diplomatic, information, and economic levers, while providing input on the military lever of national power. Ideally, they should be the quarterback of any GC threat-response, by tasking relevant departments to address threats based on their mandate and strengths.

Similar to the Department of National Defence (DND), the effectiveness of any other organizations listed above has its limitations. Cooperation, coordination, sharing of information and intelligence, and a WoG solution will ensure a comprehensive approach that will generate robust solutions to national security problems. This will enhance everyone's ability to project power and influence on nearly any audience that the GC wishes to target.

Pan-Domain Operations

The CAF recognizes five domains to include: Maritime, Land, Air, Space, and Cyber[75]. These domains represent a unique environment where operations can take place, with each consisting of specific properties that play a significant role in how the CAF can conduct operations. The addition of space and cyber is relatively recent; recognizing the emergence and importance of these two domains as research, innovation, and technology have advanced. The recently released Pan-Domain Force Employment Concept (PFEC) by the CAF has sought to introduce and codify what each domain is, and how they should be integrated, coordinated, and deployed to address the range of evolving threats that Canada is expected to face today and in the

---

[73] Canadian Coast Guard, 'CCG Mandate', 16 May 2019, https://www.ccg-gcc.gc.ca/corporation-information-organisation/mandate-mandat-eng.html.

[74] Global Affairs Canada, 'Global Affairs Canada – Home', GAC, 17 September 2020, https://www.international.gc.ca/global-affairs-affaires-mondiales/home-accueil.aspx?lang=eng.

[75] National Defence, 'Pan-Domain Force Employment Concept: Prevailing in a Dangerous World' (DND Canada, 2023). 47

future. The term pan-domain chosen by Canada is in-line with other nations who use multi-domain to describe this topic.

Within the PFEC, fourteen interrelated elements have been identified to provide a conceptual foundation for how the CAF will operate in these new strategic and operational contexts[76]. They are:

1. An **Integrated Operational Approach** to act holistically against the full array of threats and challenges;
2. **Conscious Action** to send messages and create effects that are deliberate, coherent, and aligned with strategic objectives;
3. **Pan-Domain Integration** to act with synergy across the entirety of the operating environment;
4. **Whole of Government Coordination** to allow Canada to leverage all instruments of national power;
5. **Collaboration with Allies and Partners** to detect, understand, and overcome challenges with our collective strength;
6. **Spatial Coherence** to bring actions together across the entirety of the operating environment, at home and abroad;
7. **Temporal Awareness** to begin now, act rapidly, and take a long view;
8. **Artificial Intelligence Enhancement** to harness Canada's strength in this area as a source of military power;
9. **Adapted Intelligence** to meet the demands of contemporary operations;
10. **Evolved Planning and C2** to enable integration in all its forms and thrive in our environment;
11. **Modern Capability** to prevail against adversaries and operate alongside our allies and partners as a force of choice;
12. **Broad Interoperability** to allow force elements to act internally and externally to the CAF as part of a coherent whole;
13. **Operational Culture** to become an adaptive, innovative force with a competitive and risk-tolerant mindset; and
14. **Comprehensive Resilience** to protect and preserve our capacity for action.

[76] National Defence. 7

These ideas represent and encourage the broadening of awareness and change of mindset required to be successful in tomorrow's competition and conflict. Our adversaries have observed the approaches, tactics, techniques, and procedures used by the West to operate throughout the continuum from peace to conflict, and have identified vulnerabilities to interfere or interdict us, away from our conventional strengths.

With the additional domains, departing from the more physical dimensions of land, sea, and air, it is important to consider what is *ground* and what will the ground of tomorrow's conflicts look like and represent? Historically, conflicts have involved the seizing of physical terrain, or demonstrating superiority or supremacy over areas of the sky or sea. This is no longer the case as space and cyber have sought to exploit the interconnectedness of the global population and the infinite depths of space. These two domains also offer an asymmetric advantage to our adversaries who simply can't compete on the same physical and conventional level that our nations have sought to develop. Interactions with another state or group should no longer be seen as combat in the way we expect, but more in terms of engagements, where Western nations are challenged across all domains, and at all times, blurring the binary indicators of peace and war.

The role of information within the domains should also be considered. Information is an overarching element that spans, permeates, and penetrates the other five domains, and should not be considered as a sixth or tertiary domain. Actions occurring within and across each domain generate information, which can be exploited as required to enable and enhance tactical, operational, and strategic aims. Conversely, information informs, influences, and imposes itself within the domains to shape our behaviours. Information will persist alongside all activities and domains, and is therefore not unique or different enough to be given its own consideration.

The re-emergence of great power competition and authoritarian-led states and regimes have highlighted this shift, and exposed vulnerabilities in the all-domain dominance the West used to take for granted. No-longer will any state be able to exhibit total supremacy over the five domains, and must therefore accept that control or advantage over domains will be temporary, limited, and continuously contested[77]. It will require expedient recognition, decision-making, and action to exploit these windows of opportunity if we hope to affect key enemy capabilities[78].

Our adversaries also don't recognize a clear delineation between war and peace, and instead have demonstrated that they are always in an overlapping state of cooperation, competition, and conflict. This will also require a fundamental shift in how the West views engagements with these countries, necessitating a change from a campaign approach to an ongoing or *campaigning* approach. This long-term view is required to properly plan in a deliberate fashion, incorporating OGDs, aligning with other instruments of power across DIME, and ensuring the appropriate resourcing to engage in protracted strategic competition. General Stephen Townsend identifies three key facets of this campaigning approach: that armed services win battles, but WoG wins wars; the need to win the competition that precedes the conflict; and

---

[77] David G. Perkins, 'Multidomain Battle: Converging Concepts Toward a Joint Solution - ProQuest', *Washington*, no. 88 (Q1 2018): 54–55. 55

[78] David G. Perkins, 'Preparing for the Fight Tonight: Multi-Domain Battle and Field Manual 3-0', *Military Review* 97, no. 5 (October 2017): 6–13. 13

the need to compete effectively outside periods of armed conflict[79]. Ongoing and persistent campaigning across all domains will be necessary to consider and implement a wide array of creative solutions to complex problems, utilizing all elements of national power to achieve results without first resorting to military, physical, and kinetic effects.

Pan-domain operations are not a new concept but is a recognition of more innovative ways to overcome new challenges[80]. The introduction of sea power (and eventually air power) created the need to recognize these new frontiers of capability and integrate that with the land component. The introduction of space and cyber is just the latest iteration of that evolution, resulting in publications and proposals to discuss how to incorporate new capabilities into military planning and operations.

Today's military leaders must broaden their awareness, and understand the interrelations between the domains, and develop pan-domain solutions to challenges posed in their specific battlespaces. A failure for a ground-force commander to understand these relationships, strengths, and vulnerabilities will render any pan-domain advantage useless[81]. Concurrently, there can no longer be any single-domain solutions or single-domain problems. The incorporation of capabilities from other domains presents endless possibilities and force-multiplying functions to a commander, but only if they understand how they interact within the bigger picture. To highlight this, General Townsend describes what he calls the "iPhone analogy" in that, what the iPhone did was not new, but *how* it did it was what made it so successful[82]. The concept that the iPhone didn't just make calls, but provided text, internet, navigation, social networking, and more, completely revolutionized how humans communicate, interact, plan, and execute their lives. Pan-domain approaches should be no different.

There are still numerous hurdles and challenges to overcome when it comes to pan-domain adoption and integration. The need for alignment across domains within the CAF will require the elimination of single-domain blinders that have been ingrained into our individual and collective training. Tribal mentalities amongst trades and occupations (infantry vs. armour), environments (navy, air force, and army), components (regular or reserve force), and background (military, DND civilian, and contractor) will need to be broken down and merged to generate the cooperation and coordination required to be successful in the pan-domain battlespace. This concept of removing blinders also extends to the departments within the GC. WoG involvement and interaction to tackle problems will require creative solutions that naturally spillover into OGDs, which will necessitate a change in culture and mindset to enable effective cooperation. Legal implications for the newest domains (space & cyber) will also need to be deconflicted to address their global reach that has been traditionally restricted to physical effects in fixed/geo-located areas. Our reliance on complex C4ISR systems to manage our warfighting capabilities have exposed vulnerabilities to our adversaries, who are able to exploit these areas using off-the-shelf tools and at very low cost. The hardening and protection of critical capabilities must be

---

[79] Stephen Townsend, 'Accelerating Multi-Domain Operations: Evolution of an Idea', *Military Intelligence Professional Bulletin* 44, no. 4 (December 2018): 6–7. 7

[80] Shmuel Shmuel, 'Multi-Domain Battle: AirLand Battle, Once More, with Feeling', War on the Rocks, 20 June 2017, https://warontherocks.com/2017/06/multi-domain-battle-airland-battle-once-more-with-feeling/.

[81] Shmuel.

[82] Townsend, 'Accelerating Multi-Domain Operations'. 7

considered, and alternatives identified in order to compete and fight in domains where communications and networks are degraded. The fact that all domains will be contested in future engagements[83] highlights the need to undertake a critical shift in our mindset and how we approach the complex problems of today and tomorrow.

Solutions to these problems rest with the CAF's ability to educate its members on what the PFEC means for current and future planning initiatives, and how staffs must view and approach complex problems. At a tactical level, leaders must begin to break-down siloes and single-domain thinking to incorporate pan-domain and joint training opportunities into their exercises. It is also no longer relevant to assume we will have domination or superiority across all-domains and at all times. Understanding and exercising what it means to operate in a degraded environment, when local supremacy or superiority is temporary in nature, will have a profound impact on how our activities are shaped and executed, and how tactics, techniques, and procedures will be required to evolve.

The release of the PFEC is a positive first step in acknowledging and discussing a way-ahead when it comes to integrating the unique domains and specific challenges they represent. As a vision for CAF-centric planning going forward, it will require planners at all levels to broaden their awareness when it comes to the range of capabilities and means they can employ to achieve desired effects. No-longer will single-domain solutions be effective in dealing with pan-domain problems. The recognition of what the domains bring to the CAF enterprise, and the role of information in communicating and messaging our actions, will require persistent engagement, deliberate thought, and planning, and require a department-wide and WoG initiatives to realize its full potential.

Tools

The information environment represents a complex and wicked problem to comprehend, let alone act. Identifying who or what to target, and what behaviour change or effect to generate is a complicated undertaking requiring vast amounts of data, analysis, and understanding. This section will discuss some tools that can be used to approach this problem, and how their outputs can inform the creation of activities and effects to achieve strategic objectives.

The Information Environment Assessment

The information environment is comprised of direct, indirect, emerging, and potential connections[84]. Exploring, analyzing, and understanding what those connections mean and how they influence the environment the CAF operates in is important to achieving information superiority over another party. The process to do this is referred to as the information environment assessment (IEA) and comprises the "people, processes and technology to support understanding, decision-making and the application of capability in the engagement space"[85].

---

[83] Perkins, 'Multidomain Battle: Converging Concepts Toward a Joint Solution - ProQuest'. 55

[84] Robert Ehlers, 'Course Introduction: Information Environment Overview' (Powerpoint, Information Environment Advanced Analysis Course, NDHQ Carling Campus, Ottawa ON, March 2023). 9

[85] UK Ministry of Defence, 'Allied Joint Doctrine for Information Operations'. 71

Made up of an analysis and assessment phase, the IEA is explained in more detail below and visually depicted in figure 3.8.

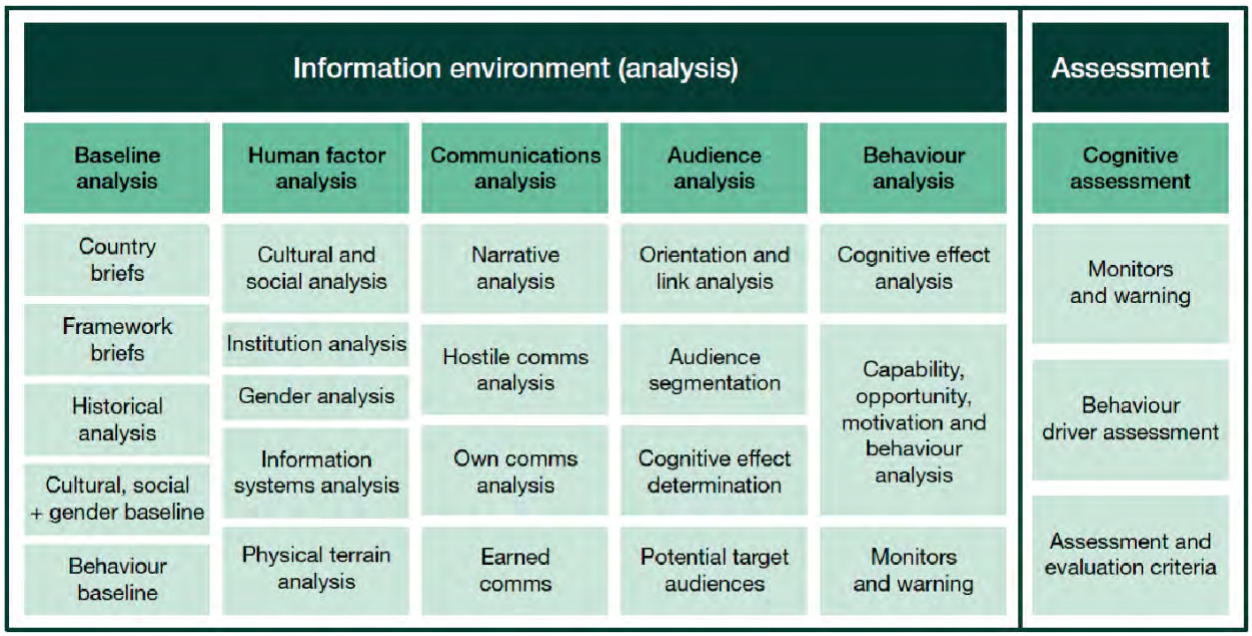


Figure 3.8: Information Environment Assessment

Source: UK Ministry of Defence, 'Allied Joint Doctrine for Information Operations'. 71

The *baseline analysis* outlines the foundational understanding to inform initial capability and force composition based on a broad study of the country, and historical, cultural, social, gender, and behavioural reference points[86]. The *human factors analysis* utilizes the PMESII (political, military, economic, social, infrastructure, and information) and ASCOPE (areas, structures, capabilities, organizations, people, and events) matrix (table 3.1) to analyze the human dimension and its effects on the operating environment[87]. *Communications analysis* looks at all actors to examine strategies, campaigns, narratives, themes, and means to communicate with audiences[88]. Military public affairs should be the champion for this and maintain the current pulse on how messages are received, perceived, distributed, and how to remain effective and relevant when communicating CAF or GC actions. *Audience analysis* looks at behaviours, attitudes, and perceptions of an audience and how that can affect a desired end-state. An audience is defined as "an individual, group or entity whose interpretation of events and subsequent behaviour may affect the attainment of the end state.' and determines how to influence their attitudes, behaviours, perceptions to achieve it"[89]. Audience analysis will be discussed in greater detail later in this paper. *Behaviour analysis* incorporates a cognitive effects

[86] UK Ministry of Defence. 71
[87] UK Ministry of Defence. 72
[88] UK Ministry of Defence. 75
[89] UK Ministry of Defence. 76

analysis to determine the social, technological, environmental, military, political, legal, economic and security levers that can be used to create a behavioural change within a target audience[90].

Collectively, the IEA is a tool used to understand the operating environment and how information is generated, transmitted, and received where CAF activities take place. There is currently no formalized method to conduct a comprehensive IEA as part of the JIPOE process in the CAF, where consideration about how activities will generate information that will be received and perceived by the various audiences involved. Greater appreciation and consideration for the role of the information environment will be an important enabler in future operations.

Table 3.1 - PMESII/ASCOPE Matrix

PMESII / ASCOPE analysis	Political	Military/security	Economic	Social	Infrastructure	Information
Area	Boundaries, districts, political party areas, ethnic or adversary strongholds	Areas of operation, boundaries, districts	Agriculture, mineral industry, economic centres, retail, offshore deposits	Religious boundaries, international governmental organizations and non-governmental organizations	Air, road, rail and river networks	Coverage for media types
Structures	Government centres, legislative, executive, and judicial (courts and prisons)	Military bases, police stations, militia, contractors	Industrial zones, technology parks, education facilities, economic centres, retail centres	Retail, sports and leisure facilities, religious buildings, meeting places	Routes, hospitals, water and power plants, education facilities, sanitation, irrigation	Communication infrastructure locations
Capability	Constitution and governance, opposition, effectiveness and corruption	Combat power, missions, intent, aims, constraints, freedoms	Industrial, agriculture, finance, markets, black market, corruption	Literacy and education levels, access to basic services, languages	Effectiveness of basic services (waste, water, power, food, health)	Literacy, data coverage, censorship, languages, outreach
Organization	Political parties, government	Police, military, security contractors	Companies, business forums, centres of learning	Ethnic groups, religions, charitable, youth, crime	Ministries, construction and maintenance facilities management, non-governmental organizations	TV, radio, Internet providers, print media, digital media, telephone coverage
People	Political leaders, diplomatic leadership	Leadership (military, police, adversary group)	Business leaders, economic governance, criminal leaders	Ethnic group leaders, religious leaders, patronage leaders, criminal leaders, influencers	Foreign investors, leadership, contractors, non-governmental organizations	Influencers, media reporters, journalists, public relations
Events	Elections, rallies, campaigns	Wars, operations, parades, anniversaries	Market days, opening hours, harvest seasons, business holidays	Religious events, key anniversaries, seasons, national holidays and events	Projects (ongoing and planned), investments, proposed closures	National censorship, campaigns, advertising, propaganda

Source: UK Ministry of Defence, 'Allied Joint Doctrine for Information Operations'. 73

Target Audience Analysis

Much like marketing and advertising, STRATCOM relies heavily on understanding not only what your message is, but who you are selling it to. Anything that the CAF says or does, or doesn't say or do creates information and sends a message. Thought must therefore be put into how that message is crafted to resonate with various audiences in order to generate the appropriate response or change in behaviour. The term target audience analysis (TAA) follows

[90] UK Ministry of Defence. 85

the same methodology of market analysis or market segmentation when trying to sell goods and services. While the formal TAA process will provide overarching direction and guidance, consideration must be made down to the soldier level about how audiences will receive and interact with each message or activity. Communicating an action or statement in only one way, will ignore multiple other groups that could be influenced by simply massaging and distributing the message in ways that will resonate with those groups.

AJP 10.1: Allied Joint Doctrine for Information Operations defines TAA as "the focussed examination of targeted audiences to create desired effects"[91]. An identified audience will likely have specific traits unique to it that incorporates demographics, behavioural characteristics, and psychographic qualities where a particular message is expected to drive a predicted outcome[92]. Quantifiable data to analyze possible audiences include traits such as: age, gender, marital status, location, education, profession, income, hobbies, media preferences, and social media platforms[93]. AJP 3.10.1: Allied Joint Doctrine for Psychological Operations further breaks down the TAA into tiers of analysis used to define and segment groups within a population[94].

Tier 1 Target Audience Analysis

Tier 1 TAA is the most detailed; it is a multi-source, scientifically verified, diagnostic methodology undertaken in-country and in the host language. It is used to identify specific latent 'behaviour'. The output of Tier 1 TAA is information *deduced* from methodically gathered data and tested against a scientifically derived hypothesis.

An example of Tier 1 TAA is a six-month contracted in-country project involving deployed field research teams.

Tier 2 Target Audience Analysis

Tier 2 TAA is any primary research involving contact with audiences which does not follow a scientifically verified deductive methodology. It may be conducted in country or remotely and is largely *'attitudinally'* based. The output of Tier 2 TAA is information *recorded* from interactions with target audiences.

An example of Tier 2 TAA is a soldier asking a local baker what he thinks might influence his neighbours to behave in a specific way.

Tier 3 Target Audience Analysis

---

[91] UK Ministry of Defence. 79

[92] Adobe Experience Cloud Team, 'How to Find and Analyze Your Target Audience', Adobe Experience Cloud, accessed 22 February 2024, https://business.adobe.com/blog/how-to/find-target-market. 2

[93] Adobe Experience Cloud Team. 6

[94] UK Ministry of Defence, 'Allied Joint Doctrine for Psychological Operations', Doctrine (NATO, September 2014). 1-4

Tier 3 TAA is the least detailed and is secondary research. The output of Tier 3 is *assumed* information.

An example of Tier 3 TAA is Internet-based research on a specific subject.

Understanding what and how an audience thinks can also inform what actions or approaches one should take. The TAA process will identify these sentiments and attitudes to inform how a force should approach the problem. A failure to properly consider an audience (or population's) feeling can result in catastrophic outcomes. During the Maryland Campaign of 1862 in the US Civil War, General Lee sought to capitalize on recent successes and march his army North into Maryland in order to isolate Washington. He assumed that the citizens of Maryland would welcome the confederacy, which turned out to not be the case. A proper audience analysis would have identified *eastern* Marylanders as sympathetic to the Confederate cause, and not the Western part of the state where his army marched through[95]. The same could be said for Russia's 2022 invasion of Ukraine, where troops were told to pack their parade uniforms for a victory parade shortly after the conflict started, expecting a warm-welcome from the Ukrainian population. Whether it was bad audience analysis, ignorance, or ego, that assessment proved to be terribly incorrect.

When the CAF communicates its actions or intentions, thought should be given to how that information is shared with domestic audiences, allied and partner audiences, adversarial audiences, and non-aligned parties. While the information regarding the activity is black and white, the way the message is crafted and delivered must be modified based on how each audience interacts with the information environment. The means and medium of delivery may also need to be accounted for to reach those audiences. Consideration should always be given to who the CAF is communicating with, and how they expect to receive and digest information.

The benefits of targeted or focussed messaging based on unique and specific audiences creates a more personalized experience that connects the receiver with those communications. The use of personas to create an accurate representation of that target audience is a useful tool in cultivating that group or following. While the CAF does consider its communications through media response lines (MRLs), statements, etc… much more could be gained by analyzing the various audiences that should consume that information and tailoring the message appropriately to further extend its reach, while promoting understanding, resonance, and engagement.

Target System Analysis

Target system analysis (TSA) is a critical part of the target development process within the joint targeting cycle. It is used to analyze not just a physical target itself, but the system of systems that enable and support that entity to be fully capable. By understanding the relationship between components of a given system, vulnerabilities can be identified and exploited to generate effects[96]. While destroying the system (ie: through kinetic effects) has been the default

---

[95] Robert R. Leonhard, *The Principles of War for the Information Age* (Novato, CA: Presidio, 1998). 36-38

[96] U.S. Air Force, 'AFDP 3-60: Targeting' (U.S. Air Force, 12 November 2021). 42

consideration or means to affect a target, the TSA process can be used to find easier and potentially more critical systems to target using other means to achieve the same result.

In an operational context, the Joint intelligence preparation of the operating environment (JIPOE) combined with the TSA approach can identify high-value targets (HVTs), high-payoff targets (HPTs), time-sensitive targets (TSTs) and target sets[97]. The production of TSAs should begin during peacetime, before the commencement of hostilities, and is accomplished through federated support and reach-back[98]. With the proper authorities, it can be possible to influence and shape environments more efficiently using this method, by avoiding striking objects or deploying troops and risking a larger or more overt action or reaction.

Figure 3.9: Elements of a Target

Source: NATO, 'AJP-3.9: Allied Joint Doctrine for Joint Targeting'. 1-17

A simple example of a TSA could involve analyzing a seaport that handles shipping and trade. In order to prevent or disrupt the proper functioning of the port, there are a number of approaches one could take to achieve that result. The first method would be employing kinetic means to destroy the port. Alternatively, a targeteer could look at exploiting cyber systems that control the cranes or vector the ground transportation for shipping containers incorrectly around the port. Space assets could be used to misdirect any GPS tracking within the shipping containers to wrong recipients or have them get 'lost' within the storage facilities at the port. Addressing the human dimension, targeting the organizations and unions that manage the employees of the port could be influenced to prevent them from working at the port (ie: a workplace dispute or strike).

[97] NATO, 'AJP-3.9: Allied Joint Doctrine for Joint Targeting', November 2021. 2-1
[98] U.S. Air Force, 'AFDP 3-60: Targeting'. 42

From an infrastructure perspective, electricity, heating/cooling/refrigeration, or the supply of petroleum, oil, and lubricants (POL) could be negatively affected to prevent the functioning of the port. Financially or economically, the executive leadership or even the stock price could be influenced and manipulated to deny the shipping of goods from unfriendly countries or force the closure of the port itself. The systems approach can take a large and complex target and break it down do its core and vulnerable components which can then be more easily exploited, influenced, or destroyed before employing kinetic or destructive effects.

The current TSA process in Canada can be very consuming both in terms of personnel and time. Given the importance of non-kinetic and non-lethal means to generate effects throughout all domains, and to avoid the threat of escalation with an adversary, it behooves Canada to anticipate and identify developing threats and invest the time to properly understand all facets of those systems. The rise of artificial intelligence (AI) to conduct the TSA process should also be explored in order to identify those vulnerabilities across multiple systems more quickly.

Narrative-Led Operational Cycle

The narrative-led operational cycle proposed by Suzanne Waldman and Sean Havel at figure 3.10 represents the synthesis of the concepts discussed so far in this paper and relates it the current operational constructs found within the CAF.

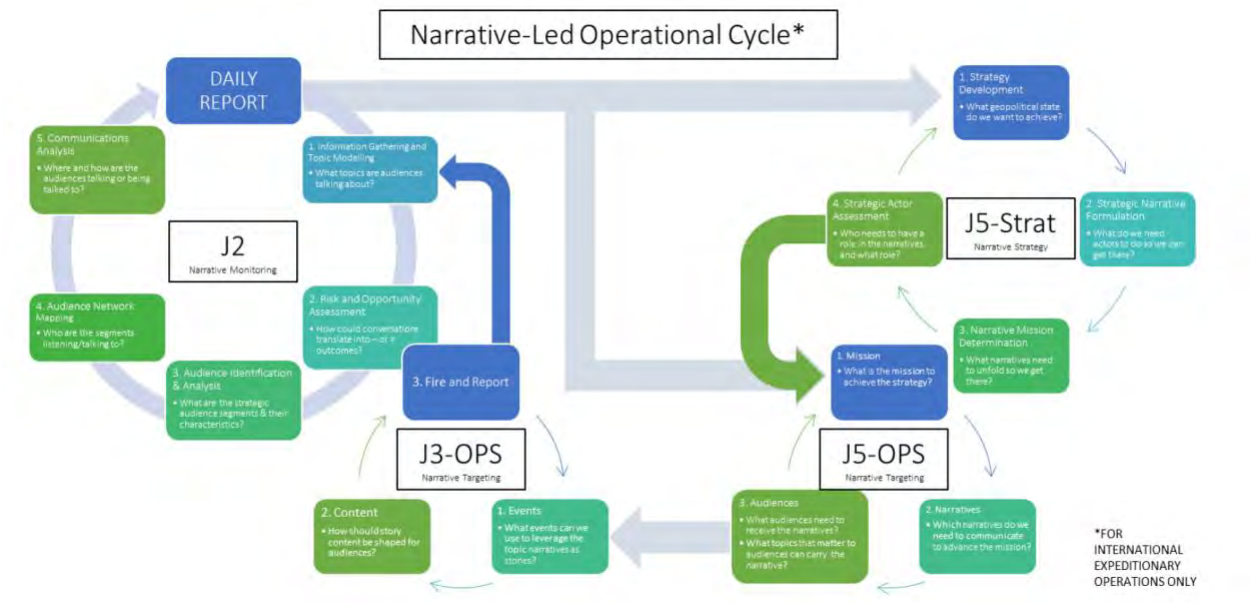


Figure 3.10: Narrative-Led Operational Cycle

Source: Waldman and Havel, ‘Updating the Concept and Execution of Narrative-Led Operations’. 4

This dynamic and iterative concept incorporates operational and planning staffs with the intelligence components to comprehensively assess, inform, adapt, and deploy narratives through events, activities, and actions, to desired audiences. Far from a "one and done" approach to operationalizing the narrative, this approach allows for ongoing analysis and adjustment of narratives and message based on near real-time feedback collected and shared by intelligence analysts. Refinement of this continuous approach will boost information sharing, appreciation for the power of the information environment, and deliver tailored effects to identified groups. Determining the effectiveness of this approach will require a greater emphasis on tracking the measures of effectiveness (MoE) of the activities undertaken, along with the adoption of new methods to track and collect data on behaviour and perception changes within the information (and non-physical) environment.

Authorities and approvals to adopt this approach should then be aligned with the existing joint targeting cycle (JTC) used by the CAF. The JTC has historically been used to assess and approve the delivery of kinetic effects on targets or adversaries but must be adapted to include non-kinetic effects in the cyber and space domains, as well as the information environment. The requirement to be timely and relevant in the information environment necessitates a targeting and approvals process to quickly deliver effects to a target audience. Instilling an approach like this into routine planning processes will familiarize and aid in the mindset shift required to be effective and competitive in the information environment. By deriving mission effects from strategic guidance, and then synchronizing the approvals and authorities processes with existing targeting working groups and boards, senior leaders will be better informed to make decisions, with minimal delay.

Distribution

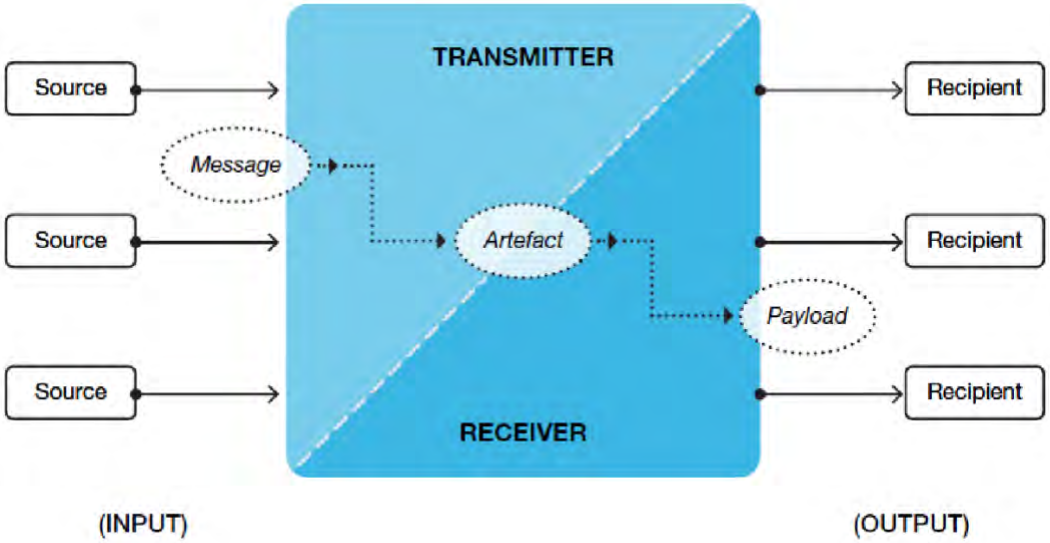
How information is presented and distributed to a target audience, is akin to the weaponeering stage of the targeting cycle. Instead of the right bomb, with the right amount of explosive, dropped at a precise location, at a precise time, to generate an intended effect, messages and information must be conceived, packaged, delivered, and received by the audience in a specific way if they are to be effective.

Governments are slowly evolving into this way of thinking, although the days of releasing carefully worded statements in press conferences, on boilerplate government web pages, or during question periods in the house of commons are still very much the way they like to do business. By doing this, they are ignoring how the population, the electorate, and their own constituents access, receive, perceive, and consume information in today's social media and short-form content environment. Simply releasing the narrative is no longer an effective strategy, and instead it must be carefully crafted, culturally relevant, in language that that audience understands, and delivered repeatedly via the means and mediums that those identified groups use regularly to access information.

The communications model at figure 3.11 and described below highlight how information travels in today's environment.

> Transmissions generally consist of user-generated content, or 'artefacts', hosted by the system. Moving from left to right … an actor ('source') posts a message on

a platform, which is published as content ('artefact') and has the result ('payload') of influencing the behaviour of someone ('recipient').[99]



Source: Model developed by GDI

Figure 3.11: The Communication Model (Global Disinformation Index)

Source: Decker, 'Adversarial Narratives: A New Model for Disinformation'. 6

Examples of payloads, and how information or narratives can be packaged within these delivery vehicles is provided at figure 3.12.

[99] Decker, 'Adversarial Narratives: A New Model for Disinformation'. 6

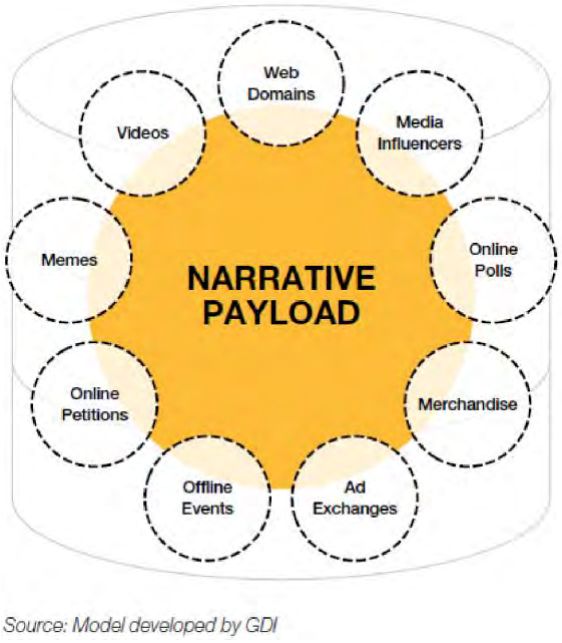


Figure 3.12: Different Elements of the Narrative Payload

Source: Decker, 'Adversarial Narratives: A New Model for Disinformation'. 7

There are a number of strategies to be effective in distributing messages within the information environment, with some detailed below:

- **Message early and often**. The first person to speak sets the narrative. This puts them in an advantageous position of deciding what is messaged, and how. The frequency of posting, and the congruence of the material can be leveraged to cultivate a dedicated following;

- **Timely and relevant**. The ability to communicate in near real-time with the audience promotes reliability and loyalty with the originator. A source that can provide engaging and interesting information first will receive more attention;

- **Volume and momentum**. Posting one statement as the authoritative message about an event does not create lasting engagement with an audience. Information needs to be shared at regular intervals, and through multiple channels and mediums to reinforce one another, while amplifying and sharing like-minded perspectives;

- **Culture and imagery**. A Western government communicating using familiar imagery and references, will not be received in the same way by a middle-eastern audience. In some cases, the messaging may actually run counter to the desired outcome and dissuade audiences from engaging with the message. Careful understanding and leveraging of cultural advisors to translate communications into payloads that will be appropriately received remains important;

- **Appropriate networks and platforms**. China and Russia use Weibo and VK respectively, not Facebook or Instagram. Distributing messages using the latter two platforms will not reach the intended audience; which therefore requires deliberate planning to gain access to the networks that audiences consume regularly if those communications are to be effective;

- **Forms of content**. Statements and press releases have their purpose, but audiences tend to consume information via many other means. One message must be able to be adapted and presented as: text (statements), video (YouTube), short form content (reels, TikTok, <10s), blogs (reddit), tweets (<280 characters), newsletters, word of mouth, etc…;

- **Overwhelm or dilute**. One source of hesitation with posting from official government accounts is the accuracy or factualness of a post, for fear that someone could disprove or refute the information. The average time to get a social media post approved at CJOC in 2023 was about 24hrs. The level of scrutiny and approval authorities were held at such a high level that achieving anything in a timely, relevant, or frequent manner was challenging. An opposite approach to this would be to post at such a volume and frequency that critics would be overwhelmed to try and fact-check or argue each post. The other benefit to this, is if something was found to be slightly inaccurate, the subsequent volume of posts would dilute the prominence of the erred message; and

- **Artificial Intelligence**. With volume and frequency comes momentum. The ability for humans to generate, maintain, and engage with the amount of content required to be effective in the information environment is exceeding that capacity. The use of AI to produce, distribute, and effect continual engagement with produced content could be a valuable tool with cultivating followings, engaging with audiences, and delivering the effects and influence that is desired.

Effective communications through the distribution of information will require a thorough understanding of the environment, the systems, the algorithms, and the audiences that have been identified. Any amount of failure to understand these areas will negatively impact the effectiveness of the communications, and in-turn the effects to be achieved. Once information has been distributed, amplification (by like-minded parties, followers, etc…), on-going engagement with the audience, and a persistent presence on that platform or in that environment will build the credibility, reliability, and therefore influence with that audience. Canada must seek to better understand and streamline the ability to distribute information quickly, tailored to the I3O effects to be achieved, if they want to be an effective and persistent presence in the information environment throughout all phases of the competition continuum.

CHAPTER 4 – CASE STUDIES

This chapter will provide examples and case studies of operations that have employed the themes and concepts presented so far. While doctrine and theory are useful, practical examples of their application provide a narrative and story that will hopefully be much easier to retain and reference. Existential crises have the habit of stressing the system to force new ideas and adopt creative solutions to solve problems. If a shift in mindset is required to employ operations in the information environment effectively, then these recent and historical examples should offer an intriguing point of view.

UK – Operation MINCEMEAT

Operation MINCEMEAT was a British plan to deceive the Germans in the Second World War about the true location of the landings in Italy. With the obvious avenue being Sicily for this landing, the British were able to convince the Nazis that the Allies would use Greece and Sardinia as their entry point, resulting in massive German troop movements away from the true objective. This was accomplished through the planting of a body on the shores of Spain with fake documents and correspondence to further support the ruse. Once discovered, the information contained with the body were conveyed to Hitler who shifted reinforcements to Sardinia and Greece. Studying MINCEMEAT highlights the importance of systems and audience analysis, narrative and storytelling, and the importance of distribution and reinforcement of the message the British were trying to send.

The body itself had to be carefully selected so that it was relatively fresh, of the correct age-range and complexion for the rank and status of the corpse and must've died from a similar cause to derive that the death was from drowning following a plane crash. In addition to the fake intelligence, a backstory and character also had to be created for the body, which included photographs and correspondence from a fiancée, a receipt for an engagement ring from a London jeweller[100], letters from his father[101], and an overdraft note from Lloyds Bank demanding payment[102]. It was also critical that the ink selected for these items would last when submerged in water[103]. Other items included ticket stubs and bills for hotel lodgings in London to construct a timeline of his movements that would support the type of intelligence he was carrying[104].

The deception documents were comprised of fake correspondence from Lieutenant General Sir Archibald Nye to General Sir Harold Alexander and Vice Admiral Lord Louis Mountbatten to Admiral of the Fleet Sir Andrew Cunningham discussing the perceived targets for the invasion[105]. These letters, along with other items were placed in an official briefcase to further lead investigators to the false intelligence.

---

[100] Denis Smyth, *Deathly Deception: The Real Story of Operation MINCEMEAT* (New York, USA: Oxford University Press, 2010). 142-43

[101] Smyth. 141-42

[102] Smyth. 123

[103] Smyth. 140

[104] Smyth. 144

[105] Michael Howard, *Strategic Deception in the Second World War* (Mackays of Chatham PLC, 1990). 89-90

In terms of audience and systems analysis, the British had already had some success during Operation BARCLAY to deceive the Germans and reinforce Hitler's concerns about a Balkan invasion[106], an unreliable ally in Italy, and the hesitation to commit additional troops to Sicily[107]. The town of Huelva in Spain was selected due to the currents and tides being favorable to the landing of a washed-up body, but also due to the known infiltration of Abwehr (German intelligence) agents and a highly competent vice-consul[108] in the area that had relatively short lines of communication to Hitler.

Distribution of the message wasn't limited to a single body or event to convince the Germans to undertake massive troop movements either. While the discovery of the body was planned to generate an organic response through a neutral country, the planted intelligence was reinforced by the creation of the fictional Twelfth Army, consisting of twelve divisions. Fake exercises, and dummy equipment was presented for observation, radio and communications traffic was prevalent (while the real headquarters in Tunis maintained relative silence), and Greek interpreters, along with Greek currency and maps were recruited and stockpiled to reinforce the belief that Greece would the target[109]. Once the body had washed ashore, pre-arranged and decodable messages were sent to highlight the accident, and the importance of recovering the body and intelligence. After it was believed that the letters had been secretly read, and returned to the envelope, additional messages were sent to indicate that the British believed the letters had not been intercepted.

What resulted was a series of events that played into Hitler's existing beliefs about ulterior landing sites for the Allies in the Mediterranean, despite urgings from his advisors and commanders. This led to reallocation of German reinforcements away from Sicily, leaving it relatively undefended. The Allies sent almost one-hundred sixty-thousand ashore in Sicily, with less than seven-thousand casualties[110] owing to the effectiveness and success of deception in Operation MINCEMEAT.

STUXNET

STUXNET was a piece of malware that infiltrated the underground Natanz nuclear facility in Iran in 2010 and targeted the centrifuges that enriched Uranium for use as fissile material for nuclear weapons[111]. The goal of the attack was to derail or delay the Iranian development of nuclear weapons[112]. Systems and audience analysis would've been used to understand the critical capabilities and vulnerabilities within their Uranium-enrichment program and were able to craft a virus that would target those specific nodes, through carefully selected vectors, to introduce the worm to Iran's systems. The origin of STUXNET is believed to have

---

[106] Macintyre, *Operation Mincemeat*. 40

[107] Howard, *Strategic Deception in the Second World War*. 92

[108] Jon Latimer, *Deception in War* (Woodstock, NY: The Overlook Press, 2001). 95

[109] Macintyre, *Operation Mincemeat*. 40

[110] Macintyre. 3

[111] James P. Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War', *Survival* 53, no. 1 (1 February 2011): 23–40, https://doi.org/10.1080/00396338.2011.555586. 23-4

[112] Josh Fruhlinger, 'Stuxnet Explained: The First Known Cyberweapon', CSO Online, 31 August 2022, https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.

come from Operation OLYMPIC GAMES under the Bush administration and continued by Obama, with the help of the Israelis[113]. This supports the theory that it originated at the nation-state level due to the level of intricacy and sophistication in its design, stealth, and types of systems it targeted.

The worm was designed to target specific programmable logic controllers (PLCs) on systems utilizing Microsoft Windows and Siemens software that were used in centrifuges within Iran's nuclear program[114]. The worm caused the motors to spin at speeds designed to sabotage the enrichment process, while containing commands that would suggest to the operators that the machines were working properly[115]. While it is believed to have infected over fifty to one-hundred thousand computers[116], it would only launch itself if specific PLC and operating systems criteria were met. Delivery of the virus relied on understanding the vectors to enter Iran's air-gapped (computer not connected to the internet) networks. Identifying individuals who worked at the facility and would be susceptible to employing outside USB-sticks (loaded with the virus) would be critical in ensuring the worm was delivered to the network.

Concealing attribution for the attack seemed to have been considered as well, with off-the-shelf code and tradecraft employed so as not to reveal the source of the worm[117]. Although once discovered, the source seemed obvious, it did allow for a level of deniability on behalf of the originator(s).

Intelligence gathering and sufficient lead time offered an alternative to the conventional method of physically destroying the facilities. Such action taken in a pre-emptive nature would have surely drawn criticism from the international community and would likely have resulted in a large number of casualties at the site. In addition, the Natanz facility was underground, making it harder to target via conventional bunker-busting bombs. By identifying smart power avenues to influence and affect the functioning of a nuclear enrichment facility in phase zero, before the capability was fully achieved by Iran, it is believed to have set the program back by at least two years[118].

Ukraine – 2022 Invasion

The current conflict in Ukraine is one of the most recent examples of how information has played a significant role in shaping the battlefield, while aiming to influence the perceptions and behaviours of the belligerents, local populations, and observers around the world. The impetus for this conflict did not suddenly arise in February 2022, but back in 2014 shortly after the Sochi Olympics.

---

[113] Fruhlinger.

[114] Farwell and Rohozinski, 'Stuxnet and the Future of Cyber War'. 24

[115] Farwell and Rohozinski. 25

[116] Thomas M. Chen and Saeed Abu-Nimeh, 'Lessons from Stuxnet', *Computer* 44, no. 4 (April 2011): 91–93, https://doi.org/10.1109/MC.2011.115. 92

[117] Farwell and Rohozinski, 'Stuxnet and the Future of Cyber War'. 27

[118] Fruhlinger, 'Stuxnet Explained'.

The invasion of Crimea by the "little green men", lacking traditional indicators of their origin, provided Russia with plausible deniability for the event while still exercising its national power and will over another sovereign country. Although the world wasn't fooled by its actions, this approach created a lot of questions about how to respond, and shed light on new tactics that would challenge how other countries view conflict, and assign attribution and responsibility.

For Ukraine, 2014 was the start of the current war taking place, and the full-scale invasion in 2022 was seen as an escalation of the conflict[119]. The initiation of the conflict drove a number of initiatives within Ukrainian society to better prepare and educate their populations on Russian intentions when it came to information warfare, and create and adapt existing organizations to deal with the threat. One of the first steps was to restrict Russian influence, disinformation, and propaganda from operating within the country. This came in the form of blocking certain television channels, expelling pro-Russian journalists, and banning social media platforms peddling Russian influence[120]. Another step was the creation of the Centre for Countering Disinformation (within the National Security and Defence Council of Ukraine) and the Centre for Strategic Communication and Information Security (within the Ministry of Culture and Information Policy) in 2021[121]. The purpose of these two organizations is to develop STRATCOM and information security management capabilities, educate the population on disinformation efforts, improve resilience within society, and fight against information terrorism[122]. A third initiative came to fruition only eight days before the invasion, when Ukrainian television networks combined to form "United News" for a daily hour-long broadcast focussed on Russian actions and conduct of the war[123]. The efforts undertaken by successive Ukrainian governments between 2014 and 2022 laid the groundwork for the actions and successes we are seeing today in this conflict's information environment. As one Ukrainian observer noted "The eight years taught us a lot. We learnt the Russia playbook, learnt the Russian narratives, the main actors, their main tricks. In February when they attacked us, we were prepared."[124].

On February 24, 2022, Russia invaded, presenting Ukrainian society with an existential crisis, and driving it into a fight for survival. The Russian invasion in 2022 was not unanticipated. Build up of Russian troops along Ukraine's borders had been happening for months leading up to February 2022. The world was watching, using a number of new technologies and approaches to stunt or derail Russia's eventual actions. This included the public release of intelligence that highlighted Russia's war plans, satellite imagery of troop dispositions and activities, and the pre-bunking of possible methods Russia may use as a justification to launch their attack (such as false-flag operations).

The Ukrainians were ready however, and quickly mobilised their armed forces and STRATCOM elements to counter Russian actions. From a communications perspective, several

---

[119] Ivar Ekman and Per-Erik Nilsson, 'Ukraine's Information Front – Strategic Communication during Russia's Full-Scale Invasion of Ukraine', *Swedish Defence Research Agency*, n.d., 97. 21

[120] Ekman and Nilsson. 53

[121] Ekman and Nilsson. 26-27

[122] Ekman and Nilsson. 26-27

[123] Ekman and Nilsson. 52

[124] Ekman and Nilsson. 66

audiences had been identified for messaging, to include: the military and defence sector, domestic society, and the international community (specifically Western-aligned nations)[125]. Narratives, themes, and messages would be crafted and distributed to these audiences, with content tailored to the effects and reactions they wanted to promote. Two main strategic narratives developed by Ukraine focus on the internal and external audience. Internally, Ukraine is framed as the underdog in the fight, but that due to Russian incompetence and poor leadership, they will prevail due to positive Ukrainian morale and resilience[126]. Externally, Ukraine's strategic narrative focusses itself as the front-line of defence for democracy and the rules-based international order[127]. As Ukraine has sought to align itself more with Western values and societies, their efforts and sacrifice to counter Russian aggression only reinforces their position.

The escalation of the conflict had an immediate effect of unifying the Ukrainian people. Events like this are able to force change quickly, and individuals are more willing and likely to sacrifice some personal freedoms and autonomy for the good of the country. Government control over the media and messaging was centralized, emerging in a "one-voice policy" or "communications pyramid" structure that rested with the country's leadership[128]. Far from hierarchical, the initial direction from government is used to set the tone for the population, and then entrusting society to lead the STRATCOM effort in a non-hierarchical and polyphonic fashion[129] (as the pyramid splays outward). The polyphonic element can be compared to a "…choir singing, strategic narratives appear to function as a leading voice that it is supported by a vast array of heterogeneous voices, navigating their own way through the song"[130]. The opposite of strict control over messaging, this approach leveraged the communications skills within the government to promote the strategic narratives from the top, while granting significant latitude to society to produce disparate messages and content that align with high-level direction.

While narratives set the strategic messaging landscape, specific themes, messages, and imagery are what drive the distribution and consumption by audiences. President Zelensky's appearance changed immediately after the invasion, from a clean-shaven politician in a suit, to a more gruff-bearded wartime leader in cargo pants and a green t-shirt. His public engagements have also highlighted him being out in Kyiv, visiting the frontlines, eating with the troops, and conducting high-profile visits to Western countries promoting Ukrainian efforts and soliciting support. To highlight the heroic sacrifices of its armed forces members, Ukraine also launched the "Defenders of Freedom" initiative which provided stories of real soldiers from the conflict to connect with human and emotional element of the war[131]. Other slogans and images have emerged both from the government and organically including "to be brave like Ukraine"[132], "it's

[125] Ekman and Nilsson. 43
[126] Ekman and Nilsson. 29
[127] Ekman and Nilsson. 29
[128] Ekman and Nilsson. 28
[129] Ekman and Nilsson. 3
[130] Ekman and Nilsson. 28
[131] Ekman and Nilsson. 30
[132] Ekman and Nilsson. 30

HIMARS o'clock"[133], St. Javelin[134], and the "Ukraine Street" initiative where streets around the world with Russian embassies have been renamed to mock their role in the conflict[135]. Efforts like these seek to provide an emotional, tragic, humorous, and relatable-human portrayal of the conflict to the identified audiences. The bottom-up creation of content, aligned with strategic narratives, represents an implicit trust between the government and their people to promote and share this conflict to generate support domestically and abroad, deter and discourage Russian action, provide levity to a horrific and tragic situation, and to overwhelm Russia's ability to gain any initiative in the information environment.

Despite all of the positives emanating from the coordination and distribution of the strategic messaging effort, the approach has introduced a number of challenges. The need for expediency in generating content and publishing it must maintain a delicate balance with the need for operational security. Troop movements, dispositions, and actions have had to be carefully considered when communicating with audiences. By decentralizing the production and distribution of the messages, an inherent trust must exist so as not to hurt or hinder Ukrainian progress during the war. Secondly, there is a need for communications to maintain the highest levels of truth and transparency as a fundamental narrative anchor point[136]. Their narrative of defending the rules-based international order depends on reliable and truthful information, while maintaining the moral high ground, so as not to sink to Russia's level.

There also remains a challenge with messaging Russian citizens, due to the extreme levels of censorship, control, and penalties associated with information that runs counter to the Russian narrative. One example of successfully messaging Russian military-aged males was through the first-person shooter game 'Counter-Strike' which had not been banned or censored by the Russian government. The game, which is played online and allows users to create their own maps to play, featured a map of a war-torn Ukrainian city, with a secret bunker containing real information and news regarding the Russian atrocities committed in Ukraine to educate a critical audience that could be called up to serve in the war in Ukraine[137]. Commissioned by a Finnish newspaper: Helsingin Sanomat, this represents a grass-roots effort to shed light and spread truthful information to an external audience experiencing extreme levels of propaganda at the hands of their government.

Lastly, the centralization and control the government demands in order to coordinate the STRATCOM effort, requires journalists to cede some level of independence and journalistic integrity for the sake of the conflict. The war, and existential crisis it has presented, has permitted this through citizens conceding personal freedoms for the betterment of the country. It

---

[133] Ekman and Nilsson. 46

[134] Saint Javelin, 'Our Story', Saint Javelin, accessed 18 January 2024, https://www.saintjavelin.com/pages/about-us-our-story.

[135] Ekman and Nilsson, 'Ukraine's Information Front – Strategic Communication during Russia's Full-Scale Invasion of Ukraine'. 70

[136] Ekman and Nilsson. 33

[137] Rich Stanton, 'This New Counter-Strike Map Was Created to Smuggle the Truth about the Ukraine War into Russia', *PC Gamer*, 3 May 2023, https://www.pcgamer.com/this-new-counter-strike-map-was-created-to-smuggle-graphic-ukraine-war-reporting-into-russia/.

will be interesting to see how programs like United News and centralized control over media entities will evolve as the conflict extends.

With the war now entering its third year, taking stock of the conflict on both sides, and navigating a path to resolution remains an important consideration for both sides. The article in The Economist by Ukraine's Commander-in-Chief General Valery Zaluzhny paints an inconvenient picture for his country and leadership as it tries to maintain morale, international support and aid, and a war machine that is experiencing sluggish progress (if any) to breakthrough Russian-occupied territory[138]. President Zelensky's "win-at-all-costs" position that Ukraine will not accept any resolution until all lands are returned and Russia is expelled, has painted him into a precarious corner, where it will be tough to pivot his message without appearing to accept a compromise with Russia. The differing views by two senior wartime leaders could be seen as a fracturing in the unity of the Ukrainian government but could also be a more subtle way of introducing potential off-ramps to the conflict without Zelensky having to reverse course on his own message. Conversely, Russia is in a position where it doesn't have to overrun Ukraine, as long as it demonstrates some amount of progress in order to frame the conflict as a 'victory' (for internal audiences at least). The next big challenge for the Ukrainian government will be how to message this stalemate, while balancing a decline in Western interest in the conflict, in order to maintain the pressure, and continue to impose costs on Russia.

For Ukraine, the eight years of conflict in Crimea and the Donbas provided an opportunity to develop and refine its strategic communications infrastructure and processes. When the invasion came on 24 February 2022, the right mechanisms were in place to thwart and counter any number of Russian attempts to overthrow the government and overrun the country in a short amount of time. A number of key themes were identified that enabled the successful conduct of strategic messaging, which included: preparation, independence, coordination, flexibility, speed, trust/reliability, tone, and transparency[139]. These tenets cannot be siloed and should be used in conjunction to enable timely and accurate information delivery to key audiences. The challenge for Western governments that are not experiencing an existential crisis, will be to educate the population on the information environments and threats during phase zero, and to put processes in place to address them now, as opposed to waiting for the catalyst of a conflict to create the urgency that will drive these eventual outcomes.

---

[138] Valery Zaluzhny, 'Ukraine's Commander-in-Chief on the Breakthrough He Needs to Beat Russia', *The Economist (Online)* (London, United Kingdom: The Economist Newspaper NA, Inc., 1 November 2023), https://www.proquest.com/docview/2884887708/abstract/ADD23819F9E44F24PQ/1?sourcetype=Magazines.

[139] Ekman and Nilsson, 'Ukraine's Information Front – Strategic Communication during Russia's Full-Scale Invasion of Ukraine'. 32,75

CHAPTER 5 – FUTURE CONSIDERATIONS

To understand the information environment is one thing, but being an effective and persistent player in this space requires addressing several hurdles and challenges. Canada's appreciation and participation in this arena has been hesitant at best, and there are a number of considerations that it must address if it is to leverage the full power of the information environment.

Structures

In order to properly shape the information environment throughout the continuum of competition, alignment across all structures within the CAF and the government writ large must be achieved. The CAF in particular recognizes the structures to enable and implement the delivery of STRATCOM and strategic effects, and has built the appropriate directorates to enable this vision.

At the strategic level, the Strategic Joint Staff (SJS) with the Director-General Strategic Effects and Readiness (DGSER) and Director of Strategic Effects and Targeting (DSET) coordinate the strategic effects frameworks (SEFs) to include narratives, while also working across OGDs to align and synchronize activities. The operational level at the Canadian Joint Operations Command (CJOC) hosts the Director of Joint Targeting and Effects (DJTE) which filters the SEFs into mission effects frameworks (MEFs) in order to inform the planning and operations staffs of the effects to be achieved during an operation. The operational level coordinates these effects with other information-related capabilities (IRCs) to synchronize the delivery of those effects. At the tactical level, the IRCs actually deploy and employ their capabilities to achieve the effects in the MEF.

While the structures exist within the CAF, what is lacking is clear and concise GC direction on what the national strategic and strategic objectives are, as well as the authorities to achieve those effects. Since the CAF occupies the "M" and portions of the "I" in the DIME construct, OGDs must be available and resourced to conduct complementary operations in the information environment from within their specific authorities. The current siloed approach creates a challenge for GC departments to act in a comprehensive and cohesive manner to achieve common end-states. In addition, if these connections are made, it is usually after a crisis has escalated beyond the point which information operations and shaping would be considered useful.

To better utilize the smart power capabilities within the GC, an overarching Strategic Effects (or STRATCOM) organization should be formed under the direction of the National Security Council (NSC) that can coordinate and synchronize all OGDs in the delivery of informational effects. Those other departments can be used to fill gaps in the CAF's ability to conduct operations (such as sanctioning a technology company from producing key components for an adversary's hypersonic missile project) or can share valuable intelligence on matters the CAF cannot collect on (such as domestic audiences). Creating that cohesive and permanent team at the GC-level could also see more broad and persistent authorities being granted to departments engaged in shaping the information environment. This proposal would still maintain the centralized planning and coordination of activities but rely on the decentralized execution

amongst OGDs and the IRCs residing within them. The centralized nature of the planning also has the added benefit of being able to coordinate strategies with allies and partners to promote and amplify communications to a much larger audience of like-minded populations.

While these structures continue to develop, it is important to note that maintaining a persistent presence in the information environment is not an episodic endeavour. Strategic effects should not be considered only after a crisis has devolved beyond a certain point, but that the information environment must be leveraged at all times in order to mitigate conflict, or at least permit the shaping of the space to make the CAF and GC's job much easier.

Policy

Policy for the CAF to operate in the information environment is still in draft. Recent missteps in how the CAF has planned and conducted activities has led to a hesitative approach on what is acceptable and, in some cases, legal. In most cases, the authorities to operate in the IE have been restrictive vice permissive, and due to the time involved in planning information operations, along with a lack of confidence in approaches, some commanders choose to eschew the IE in favour of more traditional or hard power activities. Beyond the physical policy, a fundamental shift in mindset in how the CAF and GC approach and appreciate the information environment is required.

2020 and the COVID pandemic revealed several IE-related activities undertaken by the CAF that created significant negative media attention and eroded public confidence in the institution. This included an initiative by CJOC to use the pandemic as an opportunity to test propaganda techniques on Canadians[140], and the accidental public release of documents relating to a psychological exercise in Nova Scotia, leading to a public response about packs of wolves being released into the wild by the NS Dept of Lands and Forestry[141]. This required an intervention by the Deputy Minister and CDS to provide guidance on communications activities and reign-in CAF activities in these areas[142]. This memo identified four key areas of concern with how the CAF approaches the IE:

- Lack of integration, authorities, and resources;
- Lack of doctrine/employment concepts;
- Lexicon; and
- Domestic trial and error.

---

[140] David Pugliese, 'Military Leaders Saw Pandemic as Unique Opportunity to Test Propaganda Techniques on Canadians, Forces Report Says', *Ottawa Citizen*, 27 September 2021, https://ottawacitizen.com/news/national/defence-watch/military-leaders-saw-pandemic-as-unique-opportunity-to-test-propaganda-techniques-on-canadians-forces-report-says.

[141] Brett Ruskin, 'Leaked "wolf Letter" Leaves Military Sheepish, Internal Emails Show', *CBC News*, 30 January 2024, https://www.cbc.ca/news/canada/nova-scotia/leaked-wolf-letter-nova-scotia-1.7093141.

[142] General J.H. Vance and Thomas, Jody, 'CDS/DM Planning Guidance - Enhancing Operational and Institutional Communications: Resetting Information-Related Capability Initiatives' (National Defence, 12 November 2020). 5-7

While this document has sought to reorient and codify CAF activities in the IE and with information-related capabilities, it has also introduced hesitation from Commanders to explore their use as part of their operational planning. Work continues on an Operating in the Information Environment policy, and a significant amount of effort has been made within the CAF targeting enterprise to educate the chain of command on how to effectively plan and execute activities in the IE. While progress is being made through this bottom/middle-up approach, top-down direction and guidance would greatly expedite this process.

The IE reset memo also requires some IRCs (i.e. PSYOPS, EW, Cyber) to seek GC authorities through an exercise of the crown prerogative[143]. The memorandum to cabinet (MC) process is used to grant those authorities and are usually incorporated when seeking approval for new CAF operations and deployments. It is therefore difficult identify and anticipate the specific authorities for information activities and the employment of IRCs. While the language has been included in recent MCs, it assumes a more restrictive position on their employment vice permissive.

> Seizing the initiative in the dynamic information environment requires a shift away from a defensive/reactive posture to a concerted whole-of-government approach that includes mobilizing networks and continuously updating a truthful and compelling narrative to proactively shape the debate.[144]

Acceptance and an appreciation for the effectiveness of activities in the IE have not been realized within the CAF. A lack of persistent planning and operating during phase zero results in crisis response planning which leaves limited options for comprehensive whole-of-government approaches, let alone the lead time and analysis required to develop IE capabilities. The lack of anticipation or shaping of environments mean that kinetic activities, by the forces of last resort (military), are usually the first call.

To realize the potential of the information environment and its effects on CAF and GC operations, leaders and commanders at all levels must better appreciate the force-multiplying capabilities of the information environment. This means a shifting of policies and mindsets towards persistent analysis, planning, and shaping of predicted areas of operation, centralized coordination of GC and WoG initiatives within this space, and a high level of trust in the decentralized execution of information activities to achieve timely effects to retain relevance in this fast-moving environment. The resulting policies must realize and capture the fluid nature of the IE, to create efficient processes and the delegation of authorities to the appropriate levels and permit meaningful action throughout all phases of operation and levels on the continuum of competition.

---

[143] Vance and Thomas, Jody. 11

[144] UK Ministry of Defence, 'Global Strategic Trends The Future Starts Today: 6th Edition', 2018. 16

Education

Increasing awareness about the information environment will be critical not only in understanding the reach, power, and possibilities that it can deliver from a Canadian perspective, but also the massive vulnerabilities that exist as a result of adversarial information operations against us.

From the military perspective, the United States and the United Kingdom (thru NATO) have produced comprehensive doctrine on what the IE is and how to approach it. Canada should seek to adopt existing doctrine, vice trying to define and decide on a uniquely Canadian version. A better understanding of the tactics, techniques, and procedures with analyzing the IE (using information environment analysis, target systems analysis, target audience analysis, and strategic/mission effects frameworks) will better position IO planners and the commanders that will approve them to deliver relevant effects across the battlespace. Beyond the black and white understanding of the area, anecdotal examples of IO, deception, psychological operations, space, cyber, etc… are invaluable in demonstrating the effects that these capabilities can produce without resorting to kinetic and/or lethal means.

From the civilian perspective, it is imperative that GC seek to promote the understanding and education on the ways that information have been weaponized to target our populations. Increasing citizens' resilience to mis-dis-mal (MDM) information will empower them to think critically and disregard an adversary's attempts to influence perceptions and behaviours. The Communications Security Establishment (CSE) continues to lead this effort by publishing educational materials about ways to identify MDM information. Some indicators include[145]:

- Does it provoke an emotional response?;
- Does it make a bold statement on a controversial issue?;
- Is it an extraordinary claim?;
- Does it contain clickbait?;
- Does it have topical information that is within context?;
- Does it use small pieces of valid information that are exaggerated or distorted?; and
- Has it spread virally on unvetted or loosely vetted platforms?

Beyond MDM, an understanding of the logical fallacies[146] and cognitive biases[147] that can be exploited in an audience is also important. Arguments and information presented using these

[145] Canadian Centre for Cyber Security, 'How to Identify Misinformation, Disinformation, and Malinformation'.
[146] Jesse Richardson, 'Thou Shalt Not Commit Logical Fallacies', www.yourfallacy.is.
[147] Jesse Richardson, 'Thou Shalt Not Suffer Cognitive Biases', www.yourbias.is.

tactics are attractive and appealing, and facilitate resonance of a point of view that ideally will lead to a desired change in behaviour or perception. The UK MoD have identified a similar threat in their Global Strategic Trends horizon-scanning publication, and the need for a "whole-of-society approach to defensive and offensive measures in the information space … to ensure protection against physical and cognitive attack and subversion of society, for example, through legislation and education"[148].

Going one step further, the Swedish Defence University have promulgated the Resistance Operating Concept[149] which seeks to educate the population on their roles and responsibilities in executing a "Total Defence" scenario within their national defence plan. While mainly focused on the kinetic and physical domains of resistance, it does make effort to highlight the importance of communication synchronization and STRATCOM with a focus on how to counter enemy information efforts while promoting host-nation narratives[150].

Educating the Canadian military and society writ-large on the opportunities and threats posed by the information environment will be critical in not just preventing foreign influence and interference, but also enabling the generation of smart power effects on our competitors and adversaries. While the subject matter may be triggering to a North American population that is not necessarily in the immediate shadow of an imposing and unpredictable neighbour, the importance of this type of education, indoctrination, alignment, and collaboration throughout the country pre-crisis will be imperative to ensure the greatest chances of survival.

Friendly Positioning

The techniques used by nations and actors in the information environment are not created equal. Authoritarian regimes, groups, and other who don't subscribe to the rules-based international order (RBIO) enjoy greater latitude when it comes to exploiting information in conjunction with below-threshold activities. A lack of attribution when sharing that information, and a willingness to distribute MDM-information to distort or confuse audiences, create numerous challenges for Canada to participate in the IE, and to generate the level of engagement or sensationalism as others.

Attribution remains an important consideration when generating and releasing content, regardless of the originator. An adversary may seek to conceal the identity of the originator and utilize multiple degrees of separation between it and the sender. Categories of PSYOPS and information operations are classified by *White* (products acknowledged and disseminated by the originating agency), *Grey* (products that do not specifically reveal the source), and *Black* (that appear to originate from a source other than the true one)[151]. For friendly forces, preserving credibility will usually resort to white IO, although grey and black may be considered based on the target audience and the effects desired.

---

[148] UK Ministry of Defence, 'Global Strategic Trends The Future Starts Today: 6th Edition'. 16

[149] Otta Fiala, *Resistance Operating Concept* (Stockholm: Swedish Defence University, 2019).

[150] Fiala. 43-46

[151] UK Ministry of Defence, 'Allied Joint Doctrine for Psychological Operations'. 1-6

While the differences between Canada and those actors may seem unfair, it is extremely important for the GC to maintain the moral high ground in this arena. As an ardent supporter of the RBIO, promoting truth, transparency, and factual information to all audiences must remain a key tenet of their STRATCOM approach. This requires greater consideration about what messages are being sent, a more in-depth analysis of which audiences will be communicated with, and detailed thought about what the effect is that they want to generate. These added layers of scrutiny mean that speed and timeliness of communications is put at risk.

In order to remain relevant and competitive in the IE, Canada must retain the values of legitimacy and the moral high ground, while enabling timely communications by pushing authorities to distribute messages to the lowest possible levels.

Debunking vs. Prebunking

The debate in countering adversary narratives and information relies on when is it best to initiate that fight. A battle of narratives results in a futile back and forth to maintain an audience's attention, while trying to sway behaviour and opinion in your favour. Debunking and countering existing narratives should only be considered when the shift in audience perception is so great that the investment in countering that message is necessary. Therefore, prebunking should be explored where time and intelligence is available to set the narrative early.

Debunking misinformation faces four main limitations[152]:

- False rumours spread faster through social media than information that was later revealed to be true. This is because false information can reach more people than verified information and is exacerbated by homogeneous environments or echo chambers.
- The "continued influence effect" occurs when those exposed to misinformation continue to rely on it, regardless of whether it has been debunked.
- Repeated exposure to misinformation creates the "illusory truth effect" where the constant bombardment of false data may reinforce an individual's belief in it.
- Evidence that people will respond negatively to debunking attempts and may choose to ignore factual information.

Prebunking on the other hand seeks to pre-emptively debunk avenues for misinformation by releasing factual information early to set the narrative and preventing the adversary's point of view from taking hold. There are two main components to prebunking[153]:

- A forewarning of impending attack on one's beliefs; and
- A pre-emptive refutation of the persuasive argument.

---

[152] Dr. Jon Roozenbeek and Professor Sander van der Linden, 'Inoculation Theory and Misinformation' (Riga, Latvia: NATO Strategic Communications Centre of Excellence, October 2021). 6-7

[153] Roozenbeek and van der Linden. 8

Effective prebunking was demonstrated ahead of Russia's invasion of Ukraine where the United States and British governments released intelligence about possible justifications that Russia may use to invade (i.e. false flag attacks)[154]. The types of information sharing aimed to stunt any pretext that Russia could generate, while warning audiences about the impending invasion. At one point, US Secretary of State Anthony Blinken detailed the Russian miliary plans directly to the UN Security Council[155].

While prebunking should be seen as more effective than debunking, it relies on the timely declassification of potentially sensitive intelligence, and clear communication to target audiences. The importance of this approach in phase zero should also be considered as a way to shape environments and craft factual and intriguing narratives for target audiences.

[154] Greg Myre, 'As Russia Threatens Ukraine, the U.S. "pre-Bunks" Russian Propaganda', *NPR*, 8 February 2022, sec. National Security, https://www.npr.org/2022/02/08/1079213726/as-russia-threatens-ukraine-the-u-s-pre-bunks-russian-propaganda.

[155] Laura Kelly, 'Blinken Details Russian Military Plans at UN Security Council Meeting | The Hill', The Hill, 17 February 2022, https://thehill.com/policy/international/594729-blinken-details-russian-military-plans-at-un-security-council-meeting/.

CHAPTER 6 – CONCLUSION

> *We must realize that as a nation everything we say, everything we do, and everything we fail to say or to do, will have its impact in other lands. It will affect the minds and wills of men and women there.*
>
> – Dwight D. Eisenhower[156]

Canada is already enduring relentless attacks and competition in the information environment from adversarial states and non-state actors. Because these events occur below the threshold of conventional conflict that we expect to see and react to, we are unprepared to respond, let alone actively compete in this space. The IE has affected the technological advantages and exquisite high-end warfighting capabilities held by the West, in favour of data, social media, and audiences being weaponized to achieve effects without ever having to fire a shot. The IE is the battleground of today, and is not geographically constrained, nor does it need to differentiate itself between peacetime or war.

Success in operating in the information environment requires a shift in mindset when it comes to planning all activities undertaken by the CAF. This change starts with a knowledge, understanding, and appreciation of the immense power that information and communications have with today's audiences and how our actions and inactions serve to shape the behaviours, perceptions, and attitudes of those groups. The realization that these considerations need to be recurring, especially in phase zero, regardless of a deliberate crisis or operation will be critical to the success of the CAF going forward. As stated earlier in this paper, Canada is part of an outdated approach that desires "…to excel at high-end warfare over confrontations which may fall short of violence"[157]. Realizing that we are already in a hybrid conflict with emerging great powers should drive this shift. Failing to consider these impacts poses risks to forces and missions at home and abroad.

Policy and doctrine will play an important role in defining the environment and providing a framework for how planning and operations are to occur, but it will not instill the inherent and subconscious analysis required by all soldiers to actively participate in the IE. Canada must look at adopting existing NATO STRATCOM, information operations, and psychological operations doctrine to begin formalizing the tactics, techniques, and procedures required to be effective and interoperable with our allies. Educating the force, and seeking coordination between OGDs, and GC about this environment will instill and formalize this new approach and way of thinking. Synchronization of all departments and levers of power under an umbrella organization such as the National Security Council will guarantee the best use of limited resources, while ensuring the delivery of comprehensive and concentrated effects on targets.

---

[156] Kenneth A. Osgood, 'Form before Substance: Eisenhower's Commitment to Psychological Warfare and Negotiations with The...', *Diplomatic History* 24, no. 3 (Summer 2000): 405, https://doi.org/10.1111/0145-2096.00225.

[157] Bebber, 'Information War and Rethinking Phase 0'. 42

Success will depend on the centralization of planning and aligning these operations at the highest level, while enabling and authorizing their ongoing execution at the lowest levels.

Deliberate thought must be instigated now to analyze all CAF and GC relationships worldwide to identify opportunities to cooperate and compete with, and to challenge those audiences. Taking stock of this will help guide which relationships we need to nurture, modify, or sever for the benefit of Canadian interests. Crafting narratives that are reflective of Canada's values, communicate our strategic aims, and resonate with identified audiences remains of paramount importance. The mindset shift away from capability-based planning to effects-based or even narrative-based planning; to consider how words and actions are demonstrated and communicated to various audiences to generate effects, is how this will be achieved.

The rapid of evolution of communications and technology will continue to pose challenges for governments trying to stay on top of that curve. The current GC and CAF approaches to operating in the information environment are antiquated and quickly proving irrelevant in this space. When it is easier to drop a bomb than to send a tweet, we have failed to anticipate the threat, and apply the rigor required to achieve the effect in phase zero or to consider the non-kinetic means to prosecute the target. World War III may already be underway based on the actions taken by our adversaries, but because they haven't occurred in the overt, physical, or kinetic domains, Canada (and the West) may not recognize or accept it. An organizational shift in mindset and processes is required to adopt an ongoing and persistent level of analysis and planning to capitalize on information, communication, and smart power levers to compete in phase zero and below the level of armed conflict. Concepts and tools to accomplish this have been introduced in this paper, what is now required is the understanding, appreciation, creativity, authorities and resources to approach this problem in a more effective and efficient way.

BIBLIOGRAPHY

Adobe Experience Cloud Team. 'How to Find and Analyze Your Target Audience'. Adobe Experience Cloud. Accessed 22 February 2024. https://business.adobe.com/blog/how-to/find-target-market.

Associated Press. 'Canada Military Plane Returns after Haiti Surveillance'. AP News, 8 February 2023. https://apnews.com/article/politics-united-states-government-canada-haiti-5cb8170ce19eabe133e08ae0dbbcb2a4.

Bebber, R. 'Information War and Rethinking Phase 0'. *Journal of Information Warfare* 15, no. 2 (2016): 39–52.

Canadian Centre for Cyber Security. 'How to Identify Misinformation, Disinformation, and Malinformation'. Canadian Centre for Cyber Security, 23 February 2022. https://www.cyber.gc.ca/en/guidance/how-identify-misinformation-disinformation-and-malinformation-itsap00300.

Canadian Coast Guard. 'CCG Mandate', 16 May 2019. https://www.ccg-gcc.gc.ca/corporation-information-organisation/mandate-mandat-eng.html.

Canadian Security Intelligence Service. 'CSIS Mandate', 30 April 2018. https://www.canada.ca/en/security-intelligence-service/corporate/mandate.html.

Chen, Thomas M., and Saeed Abu-Nimeh. 'Lessons from Stuxnet'. *Computer* 44, no. 4 (April 2011): 91–93. https://doi.org/10.1109/MC.2011.115.

Cooper, Alan, Robert Reimann, and David Cronin. *About Face 3: The Essentials of Interaction Design*. Indianapolis, IN: Wiley Publishing, 2007.

Cullen. 'Russian Soldier Accidentally Gives Away Ukraine Location with Geo-Tagged Instagram Selfies'. Independent.ie, 5 August 2014. https://www.independent.ie/entertainment/russian-soldier-accidentally-gives-away-ukraine-location-with-geo-tagged-instagram-selfies/30485060.html.

Decker, Ben. 'Adversarial Narratives: A New Model for Disinformation'. UK, August 2019. https://www.disinformationindex.org/.

Ehlers, Robert. 'Course Introduction: Information Environment Overview'. PowerPoint presented at the Information Environment Advanced Analysis Course, NDHQ Carling Campus, Ottawa ON, March 2023.

Ekman, Ivar, and Per-Erik Nilsson. 'Ukraine's Information Front – Strategic Communication during Russia's Full-Scale Invasion of Ukraine'. *Swedish Defence Research Agency*, n.d., 97.

Farwell, James P., and Rafal Rohozinski. 'Stuxnet and the Future of Cyber War'. *Survival* 53, no. 1 (1 February 2011): 23–40. https://doi.org/10.1080/00396338.2011.555586.

Fiala, Otta. *Resistance Operating Concept*. Stockholm: Swedish Defence University, 2019.

Finlayson, Mark A., and Steven R. Corman. 'The Military Interest in Narrative'. *Sprache Und Datenverarbeitung (International Journal of Language Data Processing)* 1, no. 2 (2013): 173–91.

Fruhlinger, Josh. 'Stuxnet Explained: The First Known Cyberweapon'. CSO Online, 31 August 2022. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.

General / Général Wayne Eyre [@CDS_Canada_CEMD]. 'Conversations on Diversity, Inclusion, and Culture Change Are Not Incompatible with Our Thirst for Operational Excellence. I Count on My Senior Leaders to Champion Culture Change. Diversity Makes Us Stronger, Inclusion Improves Our Institution. We Are #StrongerTogether - ArtMcD Https://T.Co/y4piRhtW3N'. Tweet. *Twitter*, 11 February 2021. https://twitter.com/CDS_Canada_CEMD/status/1359743611349438464.

Global Affairs Canada. 'Global Affairs Canada – Home'. GAC, 17 September 2020. https://www.international.gc.ca/global-affairs-affaires-mondiales/home-accueil.aspx?lang=eng.

Hoffman, Frank G. 'Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges'. *Prism : A Journal of the Center for Complex Operations* 7, no. 4 (November 2018): 30–47.

Howard, Michael. *Strategic Deception in the Second World War*. Mackays of Chatham PLC, 1990.

Humphrey, Aaron. 'User Personas and Social Media Profiles'. *Persona Studies* 3, no. 2 (13 December 2017): 13–20. https://doi.org/10.21153/ps2017vol3no2art708.

Kelly, Laura. 'Blinken Details Russian Military Plans at UN Security Council Meeting | The Hill'. The Hill, 17 February 2022. https://thehill.com/policy/international/594729-blinken-details-russian-military-plans-at-un-security-council-meeting/.

Latimer, Jon. *Deception in War*. Woodstock, NY: The Overlook Press, 2001.

Leonhard, Robert R. *The Principles of War for the Information Age*. Novato, CA: Presidio, 1998.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare: China's Master Plan to Destroy America*. Medina University Press International, 2021.

Litvinova, Dasha. 'How the Kremlin Weaponized Russian History - and Has Used It to Justify the War in Ukraine'. CTVNews, 21 February 2024. https://www.ctvnews.ca/world/how-

the-kremlin-weaponized-russian-history-and-has-used-it-to-justify-the-war-in-ukraine-1.6777119.

Macintyre, Ben. *Operation Mincemeat*. 1st ed. Harmony Books, 2010.

Merriam-Webster. 'Definition of IMPOSE', 16 March 2024. https://www.merriam-webster.com/dictionary/impose.

Merriam-Webster. 'Definition of INFLUENCE', 16 March 2024. https://www.merriam-webster.com/dictionary/influence.

Merriam-Webster. 'Definition of INFORM', 17 March 2024. https://www.merriam-webster.com/dictionary/inform.

Ministry of Defence GB [@DefenceHQ]. 'Latest Defence Intelligence Update on the Situation in Ukraine – 23 April 2024. Find out More about Defence Intelligence's Use of Language: Https://Gov.Uk/Government/News/Defence-Intelligence-Communicating-Probability #StandWithUkraine UA Https://T.Co/PE81EXaY81'. Tweet. *Twitter*, 23 April 2024. https://twitter.com/DefenceHQ/status/1782682068214063215.

Myre, Greg. 'As Russia Threatens Ukraine, the U.S. "pre-Bunks" Russian Propaganda'. *NPR*, 8 February 2022, sec. National Security. https://www.npr.org/2022/02/08/1079213726/as-russia-threatens-ukraine-the-u-s-pre-bunks-russian-propaganda.

National Defence. 'Canada Deploys CP-140 Long-Range Patrol Aircraft to Support Haiti'. News releases. Government of Canada, 5 February 2023. https://www.canada.ca/en/department-national-defence/news/2023/02/canada-deploys-cp-140-long-range-patrol-aircraft-to-support-haiti.html.

———. 'Pan-Domain Force Employment Concept: Prevailing in a Dangerous World'. DND Canada, 2023.

NATO. 'AJP-3.9: Allied Joint Doctrine for Joint Targeting', November 2021.

Nissen, Thomas Elkjer. 'Narrative Led Operations'. *Militært Tidsskrift (Norwegian Military Journal)* 141, no. 4 (January 2013): 67–77.

Nye, Joseph S. 'Soft Power: The Evolution of a Concept'. *Journal of Political Power* 14, no. 1 (2 January 2021): 196–208. https://doi.org/10.1080/2158379X.2021.1879572.

Osgood, Kenneth A. 'Form before Substance: Eisenhower's Commitment to Psychological Warfare and Negotiations with The...' *Diplomatic History* 24, no. 3 (Summer 2000): 405. https://doi.org/10.1111/0145-2096.00225.

Perkins, David G. 'Multidomain Battle: Converging Concepts Toward a Joint Solution - ProQuest'. *Washington*, no. 88 (Q1 2018): 54–55.

———. ‘Preparing for the Fight Tonight: Multi-Domain Battle and Field Manual 3-0’. *Military Review* 97, no. 5 (October 2017): 6–13.

Petersen, Matt. ‘Competition and Decision in the Gray Zone: A New National Security Strategy’. The Strategy Bridge, 20 April 2021. https://thestrategybridge.org/the-bridge/2021/4/20/competition-and-decision-in-the-gray-zone-a-new-national-security-strategy?format=amp.

Pugliese, David. ‘Military Leaders Saw Pandemic as Unique Opportunity to Test Propaganda Techniques on Canadians, Forces Report Says’. *Ottawa Citizen*, 27 September 2021. https://ottawacitizen.com/news/national/defence-watch/military-leaders-saw-pandemic-as-unique-opportunity-to-test-propaganda-techniques-on-canadians-forces-report-says.

Richardson, Jesse. ‘Thou Shalt Not Commit Logical Fallacies’. Poster, 2020. www.yourfallacy.is.

———. ‘Thou Shalt Not Suffer Cognitive Biases’. Poster, 2020. www.yourbias.is.

Roozenbeek, Dr. Jon, and Professor Sander van der Linden. ‘Inoculation Theory and Misinformation’. Riga, Latvia: NATO Strategic Communications Centre of Excellence, October 2021.

Royal Canadian Mounted Police. ‘About the RCMP | Royal Canadian Mounted Police’, 31 October 2019. https://www.rcmp-grc.gc.ca/en/about-rcmp.

———. ‘Commissioner’s Mandate Letter’. Royal Canadian Mounted Police. Accessed 17 January 2024. http://rcmp.ca/en/corporate-information/commissioners-mandate-letter.

Ruskin, Brett. ‘Leaked “wolf Letter” Leaves Military Sheepish, Internal Emails Show’. *CBC News*, 30 January 2024. https://www.cbc.ca/news/canada/nova-scotia/leaked-wolf-letter-nova-scotia-1.7093141.

Saint Javelin. ‘Our Story’. Saint Javelin. Accessed 18 January 2024. https://www.saintjavelin.com/pages/about-us-our-story.

Shmuel, Shmuel. ‘Multi-Domain Battle: AirLand Battle, Once More, with Feeling’. War on the Rocks, 20 June 2017. https://warontherocks.com/2017/06/multi-domain-battle-airland-battle-once-more-with-feeling/.

Smyth, Denis. *Deathly Deception: The Real Story of Operation MINCEMEAT*. New York, USA: Oxford University Press, 2010.

Stanton, Rich. ‘This New Counter-Strike Map Was Created to Smuggle the Truth about the Ukraine War into Russia’. *PC Gamer*, 3 May 2023. https://www.pcgamer.com/this-new-counter-strike-map-was-created-to-smuggle-graphic-ukraine-war-reporting-into-russia/.

Sylvestre, Bradley. ‘A Typology for Engaging in the Information Environment: Inform, Influence, Impose Operations (I3O)’. *On Track: Conference of Defence Associations Institute* 28 (June 2022): 13–18.

The Associated Press ·. ‘Fitness Devices May Reveal Sensitive Info about Soldiers’ Locations | CBC News’. CBC, 29 January 2018. https://www.cbc.ca/news/science/fitbit-privacy-1.4508382.

Townsend, Stephen. ‘Accelerating Multi-Domain Operations: Evolution of an Idea’. *Military Intelligence Professional Bulletin* 44, no. 4 (December 2018): 6–7.

UK Ministry of Defence. ‘Allied Joint Doctrine for Information Operations’. Doctrine. NATO, January 2023.

———. ‘Allied Joint Doctrine for Psychological Operations’. Doctrine. NATO, September 2014.

———. ‘Allied Joint Doctrine for Strategic Communications’. Doctrine. NATO, March 2023.

———. ‘Global Strategic Trends The Future Starts Today: 6th Edition’, 2018.

———. ‘Ministry of Defence (@DefenceHQ)’. X (formerly Twitter), 24 April 2024. https://twitter.com/defencehq.

U.S. Air Force. ‘AFDP 3-60: Targeting’. U.S. Air Force, 12 November 2021.

US Department of Defense. ‘US JP 3-0: Joint Operations’. US Department of Defense, 11 August 2011.

US Joint Force Development. ‘Competition Continuum’. Doctrine Note. US Joint Chiefs of Staff, 3 June 2019.

VAdm / vam Bob Auchterlonie [@Comd_CJOC_COIC]. ‘MGen Peter Scott, CJOC Chief of Staff, Recently Observed CAF Assistance to the Polish-Led Combat Medical Training, Vital to Ensuring the Survival of Ukrainians Fighting to Regain Their Territory. One Part of Canada’s Ongoing Support to Bring Victory for Ukraine. Https://T.Co/bygKFB4wEY’. Tweet. *Twitter*, 8 June 2023. https://twitter.com/Comd_CJOC_COIC/status/1666794825478295555.

———. ‘The Battle of Bakhmut Has Been the Longest Battle in Russia’s Invasion. Thanks to the Steadfast Ukrainian Defenders, Russian Forces Were Exhausted While Ukrainian Forces Achieved Other Strategic Objectives and Evacuated as Many Civilians as Possible.’ Tweet. *Twitter*, 5 June 2023. https://twitter.com/Comd_CJOC_COIC/status/1665721414228275200.

Vance, General J.H., and Thomas, Jody. 'CDS/DM Planning Guidance - Enhancing Operational and Institutional Communications: Resetting Information-Related Capability Initiatives'. National Defence, 12 November 2020.

Wald, Charles F. 'New Thinking at USEUCOM: The Phase Zero Campaign'. *Joint Forces Quarterly* 43, no. 4 (October 2006): 72–75.

Waldman, Suzanne, and Sean Havel. 'Launching Narrative into the Information Battlefield'. *Connections: The Quarterly Journal* 21, no. 2 (2022): 111–22.

———. 'Updating the Concept and Execution of Narrative-Led Operations'. International Command and Control Institute, 2021. https://docs.google.com/document/d/1YBuZmVmaykJoiW5Ayo5bFTjhiBfVjIFx/edit?ouid=105033277463331689685&rtpof=true&sd=true&usp=sharing.

Wardle, Claire. 'Understanding Information Disorder'. First Draft News, 22 September 2020. https://firstdraftnews.org/long-form-article/understanding-information-disorder/.

Wilson, Ernest J. 'Hard Power, Soft Power, Smart Power'. *The ANNALS of the American Academy of Political and Social Science* 616, no. 1 (1 March 2008): 110–24. https://doi.org/10.1177/0002716207312618.

Zaluzhny, Valery. 'Ukraine's Commander-in-Chief on the Breakthrough He Needs to Beat Russia'. *The Economist (Online)*, London, United Kingdom: The Economist Newspaper NA, Inc., 1 November 2023. https://www.proquest.com/docview/2884887708/abstract/ADD23819F9E44F24PQ/1?sourcetype=Magazines.