B-GA-405-000/FP-001

CANADIAN FORCES

AEROSPACE SHIELD DOCTRINE

National Defence Défense nationale

Canada

Issued on the authority of the Commander of the Royal Canadian Air Force

Commander 2 Canadian Air Division /
Air Force Doctrine and Training Division
Winnipeg, Manitoba
R3J 3Y5

ISBN: D2-297/2012E-PDF 978-1-20012-5

B-GA-405-000/FP-001

This publication is available on the DIN at: http://trenton.mil.ca/lodger/CFAWC
and on the Internet at : www.rcaf-arc.forces.gc.ca/cfawc/index_e.asp

Published by Canadian Forces Aerospace Warfare Centre
Production Section

1st Edition, February 2012

CANADIAN FORCES

AEROSPACE SHIELD DOCTRINE

PREFACE

This manual provides operational level doctrine for the Shield function of the Royal Canadian Air Force (RCAF). While intended primarily for the operational level, it also describes fundamentals applicable at the strategic and tactical levels. This manual has been designed for use by the following:

a. Canadian Forces (CF) schools and academies that train, indoctrinate, and develop personnel in the sustainment and support of aerospace operations and activities;

b. CF aerospace units and headquarters; and

c. other CF elements proposing to command or support CF aerospace forces.

This manual is presented in three chapters:

a. **Chapter 1 – Fundamentals.** Provides brief history and introduces the Shield function as one of the prime RCAF functions.

b. **Chapter 2 – Shield Function**. Explains the three domains of Shield and the interdependencies with the other RCAF functions.

c. **Chapter 3 – Application of the Shield Function**. Describes the general mechanics of dealing with Shield issues.

The manual is to be used in conjunction with:

a. B-GA-400-000/FP-000, *Canadian Forces Aerospace Doctrine*, 2nd ed.;

b. B-GA-401-000/FP-000, *Canadian Forces Aerospace Command Doctrine*;

c. B-GA-402-000/FP-001, *Canadian Forces Aerospace Sense Doctrine*;

d. B-GA-403-000/FP-001, *Canadian Forces Aerospace Shape Doctrine* (to be promulgated);

e. B-GA-404-000/FP-001, *Canadian Forces Aerospace Move Doctrine*;

f. B-GA-405-001/FP-001, *Aerospace Force Protection Doctrine*;

g. B-GA-406-000/FP-001, *Canadian Forces Aerospace Sustain Doctrine*;

h. B-GA-407-000/FP-001, *Canadian Forces Aerospace Generate Doctrine* (to be promulgated);

i. B-GJ-005-300/FP-001, *Canadian Force Joint Publication (CFJP) 3.0 Operation*;

j. B-GJ-005-314/FP-000, *CF Joint Force Protection Doctrine*; and

k. B-GJ-005-500/FP-000, *CFJP 5.0, The Canadian Forces Operational Planning Process (OPP)*.

Recommendations for amendments to this publication are welcome and should be forwarded to the Canadian Forces Aerospace Warfare Centre (CFAWC), attention: Doctrine Development Branch.

The Commander 2 Canadian Air Division (2 Cdn Air Div) is the ratification authority for this doctrine.

KEYNOTES

These keynotes are the fundamental beliefs upon which this doctrine publication is built.

- Shield is a global function.
- Shield is a fundamental enabler of aerospace power, and every member of the RCAF plays a vital role.
- Shield encompasses active, passive, and reactive measures.
- Shield is an inherent responsibility of Command.
- The development of high-level Shield policies/plans, and the control of specialized resources must be centralized. To ensure the effective protection of aerospace forces from each threat and hazard, detailed planning and execution should be decentralized.
- Shield is a function that must be continually considered by Command, Sense, Sustain, Generate, and Act (Shape/Move) while carrying out their activities.

TABLE OF CONTENTS

CHAPTER 1

FUNDAMENTALS

CF Photo: Cpl Jasper Shwartz

INTRODUCTION

Air forces exist to exercise aerospace power on behalf of the nation. This is accomplished primarily through the exploitation of the air and space environments to achieve assigned objectives. A century of air warfare has demonstrated that all effective air forces, whether they are large or small, are capable of performing a number of specific functions. These functions are influenced by the physical possibilities and limitations imposed by the environments and by each other. One cannot efficiently or effectively work without the other; however, it is the unique capabilities of each function that when integrated with the other functions ensure the proper application of aerospace power. Aligned with CF doctrine, Canadian aerospace doctrine consists of the following six functions:

Shield

The operational function that protects a force, its capabilities, and its freedom of action

COMMAND – SENSE – ACT – SUSTAIN – SHIELD - GENERATE

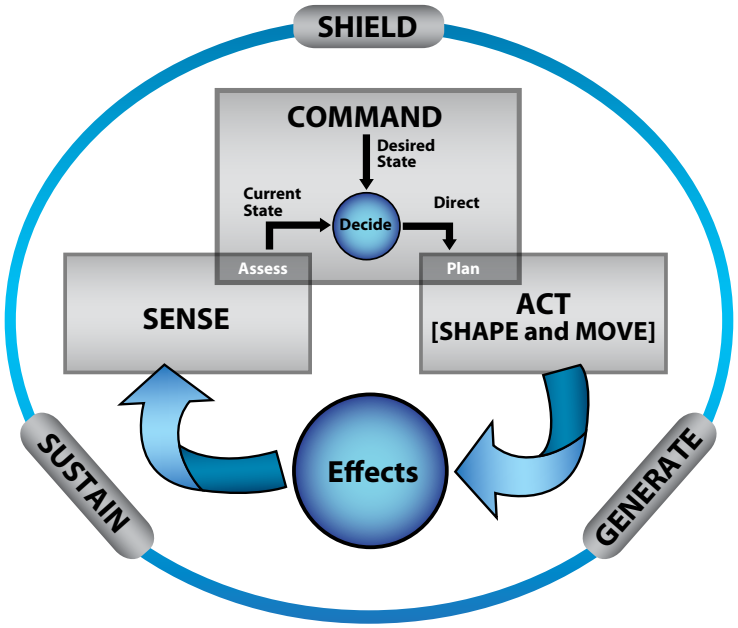

Figure 1-1. The Royal Canadian Air Force Functions[1,2]

1 The Act Function comprises the two sub-functions of Shape and Move.
2 Refer to the keystone aerospace operational doctrine handbooks for a detailed discussion of the other RCAF functions or sub-functions.

In order to conduct aerospace operations and activities, the core functions of Command, Act, and Sense operate within a continuous cycle of activities. The outputs of the Sense activities are assessed during the Command activities to determine the current state. After evaluating the current and desired states, Command activities direct and plan actions. The Act activities create effects that will achieve the desired state. Sense activities assess the results of these effects, and the cycle is repeated. As well, this cycle of activities will influence—or can be influenced by—the ongoing enabling function activities of Sustain, Shield, and Generate.

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

Sun Tzu,
Chinese General and military strategist,
6th century BCE

The Sustain, Shield, and Generate activities must be performed continuously in order to effectively maintain, protect, and develop RCAF assets and capabilities. Without the activities of these functions, the Command, Act, and Sense activities could be compromised or even eliminated. Consequently, a weakness in or failure of one function will negatively impact not only the other five functions but also the force's ability to achieve a desired state.

With the foregoing brief description of the RCAF functions, this doctrine handbook will now devote its focus to the Shield function. Within the CF, Shield is the function that protects a force, its capabilities and its freedom of action.

PRINCIPLES

Shield is an enabler that assists the other functions—Command, Act (Shape/Move), Sense, Sustain, and Generate—fulfill their roles at home wings and during deployed operations by facilitating freedom of action. Shield is not only a function; it is also a state of mind, a lens per se, through which all functions must view when planning their own activities in an effort to assess what are or could become threats that can affect their operations, how to assess the possible impact of these threats, and how best to deal with them. Shield must not interfere with or negatively impact on the ability of deployed forces to execute actions that contribute to mission success. It must create a set of conditions that enhances operational effectiveness and military efficiency, while maintaining the safety and security of deployed and non-deployed personnel. In other words, Shield must strike a balance between risk avoidance and risk taking.

When looking at the history of Shield, what is seen is a mindset transition of this function from being merely a security issue with its unilateral areas of interest, to a much more integrated and dynamic function involving all levels of authority and affecting the planning and execution of all activities. Historically, the undertaking of Shield was based on the security measures of perimeter security, hazard avoidance, information firewalls, mass and firepower, passive protection, and threat assessment. The major problems with these types of measures are:

a. "**Mass, Firepower and Passive Protection**: Mass and firepower were the dominant means by which defence forces protected themselves against adversaries. Modern militaries relied on passive protection techniques (e.g., fortifications, armour, ballistic vests, bunkers, fences, etc.) as a brute-force approach to absorb the force of an impact and achieve force protection (FP). Modern and adaptive adversaries have responded to these protection methods by targeting key vulnerabilities or employing destructive weapons to counter improvements in opposing capabilities.

Figure 1-2. Airfield Force Protection

b. "**Threat Assessment**: Traditionally, threat assessment has tended to focus on a small fraction of future conflict scenarios and environments. Threat assessment is based on the forecast of an existing threat (normally provided by intelligence personnel) and an assessment of the capabilities and intent of recognized

adversaries (e.g., force-on-force engagement of combat forces). The drawback is that while threat assessment should be proactive, by necessity, it is reactive due to unforeseen events. It then becomes a linear process that is highly susceptible to short-term distortions and changing perceptions. The new reality is that defence planners need to look ahead at operating in a highly complex, urban, counter-insurgency, and interconnected cyber environment in which there will be no clearly delineated definition of 'adversary' and where there is unlikely to be a linear threat like the days of the cold war.

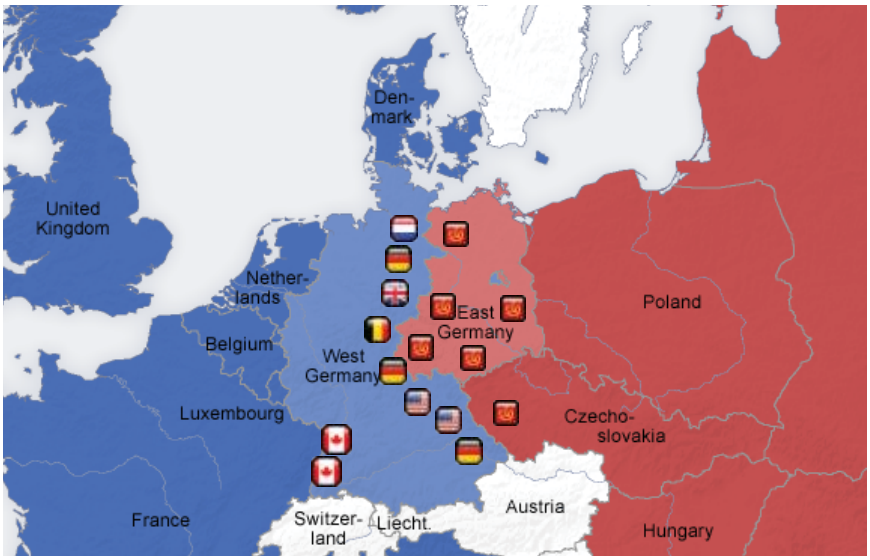

Figure 1-3. Cold War Blue on Red Map

c. "**Hazard Avoidance**: A great deal of time, effort, and defence investment has focused on avoiding large-scale, conventional battlefield hazards (e.g., chemical, biological, radiological and nuclear attack [CBRN]). Hazard avoidance, in turn, led to the stagnation and the limiting of the ability to respond effectively and quickly in our globally integrated and networked society. Techniques designed with the principle of hazard avoidance might be able to address conventional fighting situations in open country warfare, but are not designed for empowered non-state adversaries and the types of conflict environments in urban and littoral areas that will be encountered.

Figure 1-4. Force Protection Personnel Working in a Chemical, Biological, Radiological and Nuclear Environment

d. "**Information Firewalls**: The historical approach to information security was to protect the entire network(s) and system(s) against outside threats by building larger and ever more sophisticated firewalls. The underlying requirement was to have sufficient access control and user permission monitoring to protect the system. What this approach did was promote stovepiped information systems and centralized repositories that inhibited information sharing. The goal is to adopt a more proactive and anticipatory approach that exploits military, commercial, and civilian tools and networks to maximum advantage in order to leverage information faster than an adversary and to facilitate redundancy.

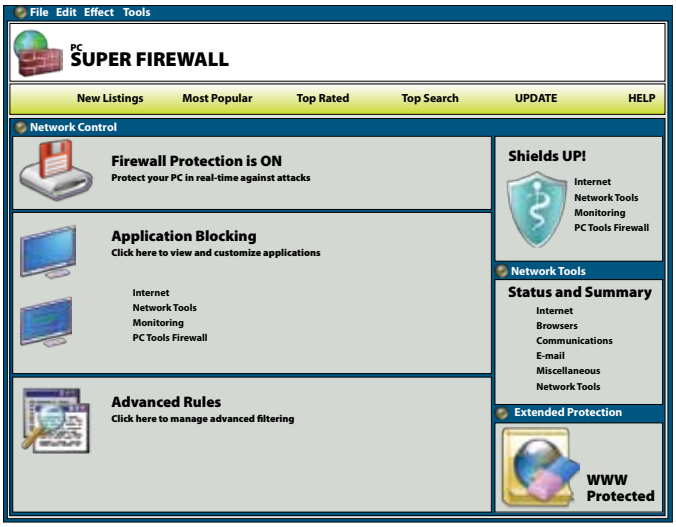

Figure 1-5. Computer System Firewall Software

e. "**Perimeter Security**: Over the course of the evolution of warfare, field fortifications have almost always resulted in a false sense of security against a swift, agile, and unpredictable adversary. The strategy of building complex defensive fortifications or concentrating military units on large bases imposes isolationist thinking that is neither sustainable nor compatible with the requirements of the local operating environment, the phenomenon of globalization, or the complex adaptive systems. The belief that an absolute bubble of security can be provided is false as it will not limit the adversary's capacity to wage an asymmetrical attack. Perimeter security measures will not eliminate all vulnerabilities and can no longer be considered as a panacea toward the avoidance of the threats of the future."[3]

Figure 1-6. Airfield Security Force (ASF)

Militaries are designed to cover a limited spectrum of operations that are constrained in function. In an operational environment, a modern military using the previously discussed measures, such as mass firepower, threat assessment, hazard avoidance, and so on, can suffer from the following restrictions:

a. These measures can be difficult to manage as they are not always fully integrated with other functions (e.g., Act and Sense). These conventional measures are not optimized to respond to the

3 Department of National Defence (DND), Defence Research and Development Canada - Centre for Operational Research and Analysis, DRDC CORA TM 2009-005, *Capability Domain Concept, Shield Capability Domain*, January 2009, 7–8 (hereafter cited as DRDC CORA TM 2009-005).

wide array of conventional and asymmetrical threats that can be encountered.

b. Using only these measures may restrict the options available to commanders, thereby impeding strategic and operational mobility.

c. The focus on these security-based methods is especially problematic in counter-insurgency or peace-support operations, where forces are required to closely interact with the local population.

d. These types of security methods are not easily scalable; they tend to be expensive to maintain and repair, and they may be seen as overly aggressive in peace-support and counter-insurgency operations.

e. Security-based methods have limited applicability in an environment that is increasingly defined by globalization and interdependence, and in environments that contain such pervasive global threats as pandemics and computer network attacks.

f. These industrial-age security methods apply primarily to the physical domain, and they offer limited ability to cope with the informational and moral domains.

g. These methods chiefly apply to Shield capabilities and will not be useful in leveraging the capabilities of a comprehensive approach that includes other military forces, civilians, other governmental departments (OGDs), non-governmental organizations (NGOs), and many others to maximum advantage.

Due to the requirement to transition from complex warfighting to stabilization activities within a single operating area, there is a need to match protection to a wide range of potential missions. This has produced a security legacy in which defensive systems have garnered the most resources with little requirement or incentive to proactively innovate or develop agile solutions. The CF mitigates threats and increases survivability by building enhanced structures, conducting vulnerability assessments, and retrofitting existing equipment with improved defensive suites. To date, this work has been heavily influenced by the classical industrial-age security model, and has ended up taking place on separate elements of the Shield system. What it has failed to do is tie together all of the Shield domains (e.g., physical, informational, and moral) in an overarching framework.

SHIELD ENVIRONMENT

"The forces of globalization are affecting the political, military, and economic world order in new, unpredictable, and potentially destabilizing ways. Patterns of conflict and their resolution will not unfold as traditionally characterized by peace, conflict, and post-conflict reconstruction activities. In certain regions of the world, failed and failing states will permeate the security landscape in our lifetime, and create the conditions for complete societal collapse. Failed states will spawn violent secessionist movements, civil and regional wars, famine, disease, and criminal predation, all of which will have spillover effects. Transnational threats, such as non-state actors, international crime syndicates, tribal, religious, and ethnic extremism and terrorism will increasingly form new sources of instability that will challenge national interests asymmetrically.

"Fuelled by radicalism and extremism, increasing competition for resources, climate change, and demographic changes, future conflict will likely be violent, protracted, and messy. The burgeoning population growth in major urban centres, particularly in areas of the developing world, will have implications for both public and private operations, as well as disruptive effects on the supporting capacity of the global economy and environment. Global competition for natural resources and environmental scarcity will trigger humanitarian disasters and the mass migration of people and refugees. Climate change will intensify the build-up of energy shortages and create further environmental and resource scarcity, as well as competition for natural resources, increasing the likelihood of failed states and terrorism.

"The ongoing proliferation of weapons of mass destruction (WMD), especially into the hands of 'rogue' states or non-state actors, will be of particular concern. Such weapons will provide non-state actors and small, radical organizations with the potential to orchestrate destructive and disruptive effects on an enormous scale. Non-state actors, who are being empowered by modern technology and weaponry, threaten to undermine the traditional strength and numerical superiority of military forces of organized nation states. These non-state actors intermingle and merge with a local population, apply non-traditional tactics, and can use our freedoms against more open societies…. Furthermore, the increase in interdependency of critical infrastructure, specifically within the key supporting sectors of finance, communications, and energy, will become a growing concern as vulnerabilities become exploited by cyber attack or brute force attack, resulting in disruption or

denial of service and unimagined cascading consequences to the national well-being."[4]

A variety of conventional and unconventional adversaries (e.g., states, non-state actors, terrorists, mercenaries, insurgent forces, irregulars, militias, multi-national groups, organized criminals, etc.) may exploit technologies, command and control systems, and information technologies. These adversaries may not be easily identified, defined, or evaluated. They can operate autonomously, intermingle with the local population, and have at their disposal highly lethal anti-access capabilities (e.g., sea-mines, volumetric munitions, and man-portable missiles and rockets) that are difficult to defend against. Conventional platforms could be particularly vulnerable to these types of weapons. "Intermingling of adversaries also provides the opportunity to influence attitudes, behaviours, and thus … allegiances...."[5] Shield requires the ability to counter purpose-built capabilities that may be employed to specifically target our vulnerabilities and gaps and challenge the CF and coalition partners asymmetrically.

Forces have had to operate in highly complex, urban, littoral, and cyber-operating environments in which there have not been clearly delineated front lines. Forces have undertaken numerous roles (combat and non-combat) in inhospitable environments ranging from mountainous terrain to densely populated urban centers and congested littoral regions. Forces may be subjected to asymmetrical attack (e.g., ambushes, improvised explosive devices [IEDs]), in addition to the normal battlefield hazards. They have confronted risks from a range of hazards, including catastrophes caused by human intervention and threats independent of human action. The Shield function should allow forces to simultaneously undertake distributed and multi-dimensional operations, from complex warfighting and stabilization activities to humanitarian and reconstruction missions, within the same mission space. This underlines the requirement for forces that are capable of withstanding the shocks, impacts and stresses encountered in the physical and moral domains, and maintain the initiative throughout or rebound quickly.

There are a number of survivability and protection challenges that may be encountered during operations. Harsh physical conditions, including extremes of temperature, noise, isolation and darkness, can challenge the physical and psychological resilience of military personnel. When combined with time pressures and difficult living conditions, these factors can contribute to an increased requirement to shield forces against non-battle-related injuries sustained during operations.

4 Shaye K. Friesen and Andrew N. Gale, "Slaying the Dragon: Future Security Environment and Limitations of Industrial Age Security," *Canadian Military Journal* 11, no.1, http://www.journal.dnd.ca/vo11/no1/07-friesen%20gale-eng.asp (accessed July 26, 2011).
5 Ibid.

The battlespace likely will continue to be joint, interagency, multinational, and public (JIMP).[6] The presence of neutrals, NGOs, OGDs, multinational corporations, contractors, academia, think tanks, and local population(s) will continue to make it difficult to differentiate adversaries from non-combatants. Expectations regarding "blue" casualties and collateral damage highlight the importance of agility and precision in the Shield system. Operations which necessitate the incorporation of other agencies and non-state actors into the Shield system can present interagency risks, including the potential for more effective manipulation of information (media, internet) and the spread of misinformation.

ASSUMPTIONS OF SHIELD

Protection of capabilities in the highly lethal, all-domain, and effects-based future operating environment requires a globally integrated, active, and layered Shield network. This network should be integrated with the shielding capabilities of other agencies and multinational partners, for example: defence forces (national and allied); intelligence agencies; OGDs; NGOs; think tanks; as well as industry and academia across the physical, informational, and moral domains. These components should be integrated as part of Shield and provide multiple and overlapping levels of redundancy (e.g., infrastructure, systems, and services). The capabilities of this network should operate as a comprehensive defence system to absorb, dilute, or otherwise distribute the effects of potential hazards.

The method by which the Shield function is employed is dictated by the following current assumptions:

a. The fundamental missions of the CF will not be changed by the Government of Canada (GoC).[7]

b. The international situation is expected to remain inherently anarchic and volatile.

c. The CF will be called upon to participate in a range of military operations as part of a multinational coalition.

d. The possibility of pursuing independent CF operations to protect vital interests cannot be ruled out.

e. CF deployments will continue to be influenced by politics, economics/budget, legal issues, and rules of engagement (ROE) consistent with

6 Peter Gizewski, Michael Rostek, and Andrew Leslie, "Comprehensive Operations: Moving to a JIMP-capable Land Force," *Vanguard* (2006), http://www.vanguardcanada.com/ComprehensiveOperationsGizewskiRostekLeslie (accessed July 20, 2011).

7 *Canada First Defence Strategy*, 12 March 2010, http://www.forces.gc.ca/site/pri/first-premier/defstra/summary-sommaire-eng.asp (accessed July 20, 2010).

Canadian laws and values, and will test the will of the Canadian public to support long-term engagement, spending, and losses.

f. There will be an expectation to minimize casualties, as well as to reduce the level of collateral damage, in future operations.

g. Recruitment, as part of Generate, will remain consistent with levels mandated by the federal government, while attrition is expected to follow historical trends.

h. The Department of National Defence (DND) / CF will maintain an internal capability and capacity to follow, apply, or rapidly exploit science and technology advances, and new knowledge and information in order to ensure an optimized capability that addresses critical mission outcomes.[8]

The expanding use of infrastructure, systems, and services in the network should supplement capabilities and agility while reducing overall risk and vulnerability. This layering effect that allows the CF to capitalize on joint interdependencies, match levels of protection to appropriate countermeasures (passive or active), and achieve greater synergies through improved situational awareness (SA), information sharing, and collaboration, cannot be obtained by protecting individual components separately. Even if one or more of the layers fail, the Shield system can still be capable of functioning as a result of the mutually reinforcing and interdependent networks, systems, and capabilities. Explicit consideration and exploitation of moral components of the Shield framework may change the way in which information is shared, how collaboration within the network occurs, and how responses to external hazards are coordinated, thus forming the basis for increased agility and precision.

The Shield function must be capable of adjusting the level of shielding to meet changing requirements, exactly where and when it is required. It is based on prioritizing what we are going to secure and rapidly deciding how we are going to protect it using vulnerability and risk-based analysis. Forces should initiate prevention, pre-emption, and deterrence operations that disrupt/interdict all forms of external hazards before they pose a risk. By leveraging information and assets, applying a vulnerability and risk-analysis-based approach, and exploiting intelligent and predictive tools, the end state can be a much more adaptive and focused Shield function that is customized to particular hazards and vulnerabilities. Implicit in this function is recognition that the CF can depend on other entities (e.g., NGOs, non-state actors) for critical capability, information and

8 DRDC CORA TM 2009-005, 14.

intelligence, and that the security and protection of these external entities will be absolutely essential for mission success. The Shield function should be highly dependent on offensive action and should be closely synchronized with the Act and Sense domains. An aggressive and offensive orientation in the physical, informational, and moral domains may reduce the requirement to shield forces. However, personnel must remain vigilant, and the Shield function will always be present and able to adapt quickly to the requirements of the mission.

CHARACTERISTICS OF SHIELD

An effective Shield that meets the critical challenges of the current security environment must consist of the following characteristics.

CHARACTERISTICS
NETWORKED
AGILE
PRECISE
PERSISTENT
ROBUST
SCALABLE
INTEROPERABLE

a. "**Networked**: Must be supported by a broader community and able to incorporate multiple [levels] of processing and information to produce a collaborative, flexible, and redundant network with the ability to interface/function across the entire spectrum of operations with other agencies, including allies/NGOs/OGDs. The … Shield system must be seamlessly integrated, incorporating all components, and be capable of understanding how all partners and connections are interrelated to allow shielding effects to be provided from multiple sources.

b. "**Agile**: A real-time, adaptable, rapidly responding level of shielding with the ability to re-scope, re-scale, and reconfigure itself in response to the ever-changing continuum of potential threats…. [Forces must continue to be adaptive, flexible, innovative, and able to reconfigure] systems, organizations, and procedures according to every changing mission circumstance. The … Shield function must provide a dynamic, upgradeable, and layered shield effect incorporating modular technology and automated [and timely] intelligence. Agility connotes [that] Shield [be] highly responsive and streamlined, and characterized by the appropriate level of shielding to enable the [other functions to carry out their particular missions]. In order to be truly agile … Shield [must be enabled by] an effective learning organization.

c. "**Precise**: The [Shield function must] accurately and rapidly [tailor itself] to ensure mission accomplishment while minimizing friendly and neutral losses. [It] must possess a near-instant ability to identify, target, and neutralize the effects of [threats]. These activities must provide selective entry and exit from … Shield, and be [available] in a variety of conflict contexts (e.g., urban … and

littoral environments). Leveraging state-of-the-art technology to accurately identify a threat and negate its potential impact may reduce potential vulnerabilities and weak points, thereby instilling [in forces] confidence in [their] ability to [operate].

d. "**Persistent**: Modern and future threats can be unrelenting. A layered system with built-in redundancy must be able to operate on a near-continuous basis. The … Shield [function] … must be capable of withstanding continuous or repeated attacks, and able to continue the mission in spite of sustained injury or compromise. This system must leverage state-of-the-art technology to provide a redundant, comprehensive, and layered Shield effect.

e. "**Robust**: The [present and] future battlespace is likely to require operations in an urban/littoral environment where there is potential for interaction at close range involving highly lethal adversaries. Vulnerabilities and gaps [may] be specifically targeted in this environment…. Shield must be capable of absorbing, diluting, or otherwise deflecting these attacks in different directions while contributing to the freedom to act decisively. It must be insensitive to external stresses and adopt proactive protection measures, such as decoys, deception, and concealment in order to protect forces at close range.

f. "**Scalable**: Achieving mission success and shielding deployed forces in all environments and domains will require tailoring of the forces involved to fit the mission. A real-time, scalable system able to produce an appropriate, graduated shield effect in response to a potential threat is required. This system must generate a range of responses through maximum use of logical, ethical, and rule-based control systems."[9]

g. **Interoperable**: This involves the ability of systems, RCAF units, or Canadian Army and Royal Canadian Navy elements, to provide services to and accept services from other systems, units, or elements, and to use the services so exchanged to enable them to operate effectively together.

SHIELD WITHIN THE AEROSPACE REALM

The aerospace environment is unique and demands a distinct approach to operations within it. B-GA-400-000/FP-000, *Canadian Forces Aerospace Doctrine* identifies eleven characteristics of aerospace power. As shown in Table 1-1, Shield is essential to offset the vulnerabilities presented by five of these characteristics.

9 DRDC CORA TM 2009-005, 20–21.

Aerospace Characteristic	Definition and Vulnerability	Examples of how Shield Mitigates Vulnerability
Fragility	Aerospace vehicles tend to be more fragile than surface vehicles, and therefore require special handling to keep them in operation.	Shield provides attack warning, physical security, stand-off and hardened shelters for aircraft.
Impermanence	Typically, aerospace platforms cannot remain aloft indefinitely; they cannot hold a station permanently. This can be offset by committing aerospace platforms in rotation to maintain a posture of relative permanence, or by repeating missions as required.	Shield provides secure operating bases.
Sensitivity to Environmental Conditions	Aerospace power is typically sensitive to environmental conditions. Bad weather, for example, creates difficulties with take-offs and landings, navigation, target acquisition, and weapons delivery.	Shield warns about adverse environmental conditions and provides shelters for aircraft.
Sensitivity to Technology	Relatively small innovations in technology can have a significant impact on the effectiveness of aerospace power. Technological advances dictate an ongoing requirement for continuous improvement and development of aerospace forces.	Shield in the threat assessment phase of planning identifies enemy capabilities which are technology driven.
Support Dependency	Aerospace power requires a high level of technical and logistical support that must be provided from a support base of operations.	Shield protects technical and logistic support assets, including fuel, munitions storage, and runways.

Table 1-1. Shield Functions Mitigate Vulnerabilities

SUMMARY

This chapter introduced the Shield function keystone doctrine manual. Key to this introduction is the important fact that Shield is a state of mind within all of the other functions: Command, Act (Shape/Move), Sense, Sustain, and Generate. Looking through the Shield lens when planning and conducting activities facilitates the achievement of mission success. Shield identifies the pitfalls of conducting an operation through the use of mass firepower and passive protection, threat assessment, hazard avoidance, information firewalls, and perimeter security. To optimize the achievement of Shield, there are seven desired characteristics that should be incorporated into the planning and execution phases: networked, agile, precise, persistent, robust, scalable, and interoperable. The goal of Shield is to counteract the inherent risks within the aerospace realm of fragility, impermanence, sensitivity to environmental conditions, technology, and support dependence.

CF Photo: Cpl Asko Karhunen

CHAPTER 2

SHIELD FUNCTION

CF Photo: Cpl Jean-François Lauzé

INTRODUCTION

"Shield what? … 'Shield' … is a layered, integrated and fully dimensional function that seeks to prevent any influence of enemy forces across the physical, moral and informational planes that could affect survivability or freedom of action. In essence, Shield is a concept that includes the requirement to identify and protect the friendly force centre of gravity and its subsidiary critical vulnerabilities from attack by an adversary. In the future, Shield in the physical plane will focus on the traditional defensive concepts to include the protection of soldiers, partners and non-combatants, platforms, systems, equipment and facilities. In the informational plane, Shield will likely focus on the protection of friendly information, information products, information systems and friendly force activities. It must be acknowledged that a 'network enabled force' accrues both the benefit of an increased ability to share information and the increased risk of an adversary accessing or disrupting that same network. In the morale plane, adversaries will seek to undermine the legitimacy of our mission and our force. Simply put, they will attack our will to fight. To counter this, increased emphasis on training in the areas of ethics, mission legitimacy, resistance to psychological threats, etc. will be required." [1]

Figure 2-1. Airfield Shield

1 R. J. Hillier, Director Land Strategic Concepts, DLSC 2007-04-27 *Omni-Dimensional Shield in Future Conflicts*, 3.

COMPONENTS OF SHIELD

Shield considerations can be divided into the physical, informational, and moral domains. The physical domain is where physical elements operate and interact to achieve kinetic and non-kinetic effects. The informational domain is characterized by the use of information, electromagnetic spectrum, networked systems, and associated infrastructure. These domains also consist of several important capabilities: pre-emption, detection, assessment, warning, defence (active and passive), and recovery. The moral domain, including elements such as will, motivation, leadership, confidence, courage, fear, and fatigue, can facilitate or hinder the ability of defence forces to operate and of cognitive elements to achieve desired results. Personnel must be aware that if threats and risks are mitigated in one domain, they may still have the ability to wage asymmetrical attack and inflict damage to our forces in another domain. Only when there is a totally integrated Shield function that addresses all domains and is continually monitored, adapted, and implemented by all air force personnel, will the possibility for a successful Shield function exist.

PHYSICAL DOMAIN

Shield in the physical domain refers to both the kinetic and non-kinetic battlespace; it requires personnel to consider all physical domain issues that can affect mission effectiveness. This physical domain can include all the aspects of FP; however, it must also consider the impact they can have on the other domains within the Shield function, namely, informational and moral.

Technology has provided additional connections between physical protection measures and other personnel within the Shield function; this can increase the risk assessment/mitigation process available to senior leadership. If the process of identification, assessment, and mitigation are conducted thoroughly, it should provide a plan which details a layered and interactive approach to the physical domain by providing improved robustness and redundancy. Additionally, if this process is carried out, it can improve the SA within the physical domain itself, improve the ability to take advantage of information and intelligence, and enable effective protection within the physical domain.

In the past, the physical domain has provided overwatch, mainly with the use of personnel as a kinetic measure, and reduced footprints, camouflage, concealment, and deception (CCD) and noise discipline, as non-kinetic measures to achieve this capability. Today, these are greatly enhanced through the availability and use of high-tech equipment such as visual and audio sensors, and advanced warning networks such as the Royal

Air Force's (RAF) Big Voice.[2] A combination of tactics, techniques and procedures (TTP) in concert with high-tech equipment can enable the physical domain to provide maximum survivability while ensuring freedom of action (see Figure 2-2). However, in order for the Shield function to enable mobile and agile forces, they should be designed to adapt and survive the geographical challenges of terrain, the environment, and sociological conditions. This may result in situations in which forces could be required to operate outside the Shield threshold, for instance, to secure the allegiance of the local population in counter-insurgency operations. The interaction between kinetic and non-kinetic security measures can rely on agile decision support tools and systems that support more proactive responses. The "physical Shield includes [but is not limited to]:

a. protection against enemy ballistic, blast, and projectile effects (including air/missile attack);

b. protection from laser dazzles and the blinding effects of smoke;

c. protection from enemy information operations;

d. protection from weapons of mass destruction (e.g., [CBRN] early detection warning systems, integral platform [CBRN] systems, and soldier [CBRN] ensembles);

e. protection from active medical threats (i.e., subsequent to becoming a casualty), a condition advanced by such measures as casualty evacuation and treatment in the battlespace;

f. protection (including preventative and corrective medical treatment measures) from passive threats such as hazardous climates (e.g., extreme heat or cold, and dehydration) and environments (e.g., toxins, disease, wildlife);

g. protection against surprise. Toward this end, SA [part of the Sense function] is vital to survival across the entire battlespace. SA will enhance the soldier's ability to be proactive, avoid surprise, and thus survive. In a poorly understood situation, surprise can come from friendly forces as well as the enemy. Loss of life due to friendly fire is a reflection of inadequate Shield…. Friendly fire incidents have the potential to undermine the morale of an otherwise highly motivated combat force;

2 An airfield broadcasting system capable of broadcasting warnings and alerts over the entire airfield and camp, employed at Kandahar Airfield by the RAF regiment force protection element.

h. passive protection from detection (e.g., stealth-advanced camouflage, mobility, cloaking devices [chameleon-type] and deception); and

i. the proactive ability to apply lethal kinetic effects against a potential threat before it can engage."[3]

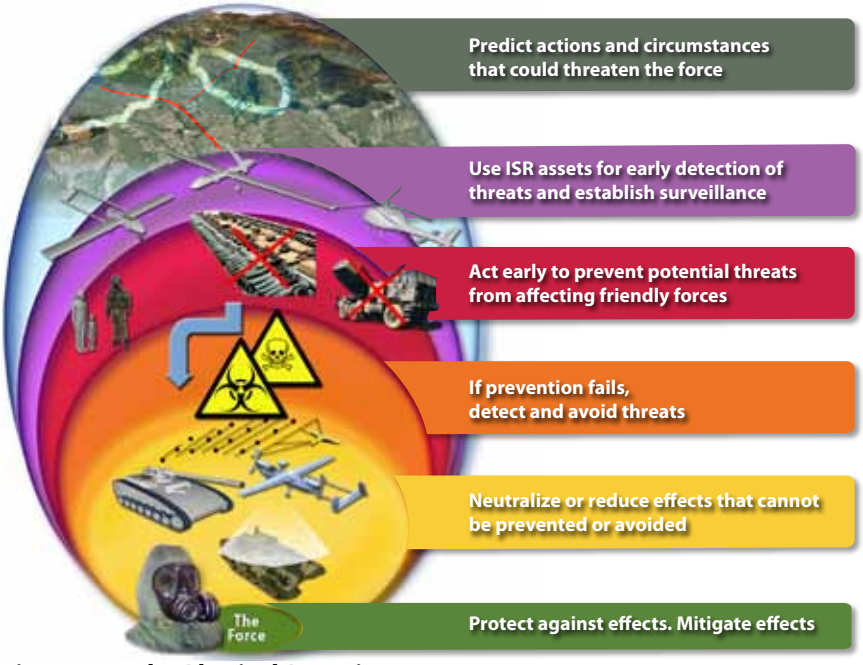

Figure 2-2. The Physical Domain

INFORMATIONAL DOMAIN

The Shield function is concerned with the protection of the informational domain and ensuring that it functions properly without interference from exterior or possibly interior influences. This also includes areas which deal with data transfer that can have adverse effects on the other functions and capabilities. Several of these areas include the Sense function and the domain of electronic warfare (EW), support of the Command function, and every other aspect of operations which can be affected by some sort of data transfer.

Sense interacts in the achievement of information superiority along with the Shield (by protecting) function and Shape (by denying the enemy) sub-function. Modern military operations are increasingly dependent on information to succeed. Information superiority is defined as "the operational advantage derived from the ability to acquire, exploit, protect

3 DND, Directorate of Land and Strategic Concepts, *Future Force Concepts for Future Army Capabilities* (Kingston, ON: 2003), 130, http://www.army.forces.gc.ca/DLCD-DCSFT/pubs/special/futureforce/FPAC_eng.pdf (accessed July 20, 2011).

and disseminate information without interruption from an adversary while denying an adversary's ability to do the same."[4] Information superiority is an objective in itself, but is also used as a descriptor to define the causal relationship between the decisions taken by friendly forces and the subsequent effect that they have on the adversaries' ability to influence the operating environment. It ultimately assists in enabling the commander not only to make better decisions, but also to anticipate and respond to changes in the operational environment faster than an adversary. Presumably, if a friendly force can achieve information superiority over an adversary, they will be able to make better decisions faster than the adversary can react and have a decisive edge in the information and operations domain. As a Shield function, it is essential to protect the information domain to enable all aspects of operations.

ELECTRONIC WARFARE

Electronic Warfare contributes to the Shield function through all three of its sub-components: electronic warfare support (ES), electronic protection (EP), and electronic attack (EA). In shielding a force, ES sensors must first detect the presence of an adversary's use of the electromagnetic spectrum in order to intercept, identify, and locate sources of electromagnetic energy. Once hostile signals are detected, ES sensors can then record those signals for detailed analysis so countermeasures can be developed and employed, further shielding RCAF assets.

While the interception of hostile electromagnetic energy can be used by friendly forces for immediate tactical purposes, such as flying outside of an adversary's radar coverage, any intentional or inadvertent transmission of friendly signals can provide similar information to an adversary, and this information can also be used to sense, locate, and ultimately target friendly forces. Therefore, the transmission of any electronic signal must be viewed as an activity which can potentially be used to target one's own forces, and measures which can reduce or eliminate emissions altogether will contribute to the shielding of friendly forces.

Electronic protection measures are employed to shield friendly forces from the degradation, neutralization, or destruction of their own electronic systems and can be either passive or active in nature. In airborne platforms, passive measures include aircraft radio frequency (RF) and infrared (IR) signature reduction, while active actions may consist of manoeuvring outside weapons engagement zones, employing active electronic jamming, using decoy systems which broadcast false signals, or the use of frequency hopping radios and radar systems which sweep through a pre-programmed, pseudo-random set of frequencies to prevent effective jamming by an adversary.

4 *Defence Terminology Bank* (hereafter cited as DTB) record 41413, http://terminology.mil.ca/term-eng.asp.

Passive and active EP measures are also used to shield ground-based electronic systems which utilize the electromagnetic spectrum (EMS) (i.e., tactical radios, cellular phones, wireless computing devices), or which radiate signals in the EMS (i.e., desktop computers, printers, fax machines, etc.). This is achieved through the use of passive measures, such as emission controls (EMCON) on communication and information systems (CIS) equipment (i.e. emission security [EMSEC] zoning, TEMPEST), electronic hardening of equipment during design and manufacturing, and the use of wartime reserves whereby the full extent of a friendly electronic system's offensive and defensive capabilities are withheld from normal use until they are required for use in war or emergency. Active RF jamming and electronic masking of friendly electromagnetic (EM) signals are also employed to proactively shield ground-based electronic systems from an adversary's EW capabilities.

While EP measures seek to shield and protect one's own use of the electromagnetic spectrum, EA measures employ electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment for the purpose of degrading, neutralizing, and/or destroying an enemy's combat capability. Anti-radiation missiles are highly effective in shielding aircraft in flight, as they are designed to home in on hostile RF signals and to either destroy the transmitting radar site, or to cause the site to cease radiating under the threat of being destroyed by an in bound missile.

Additional information on EW capabilities and employment can be found in B-GA-403-002/FP-001, *Aerospace Electronic Warfare Doctrine.*

The RCAF operates on a number of network technologies, some are more secure than others, and some are globally accessible. With accessibility comes possibility of threats to the systems. These systems are broken down into three distinct activities: computer network defence (CND), exploitation (CNE), and attack (CNA), which together form the basis of the computer network operations (CNO). Together they attempt to provide the domain with detection, protection, and counter methods to prevent attempts at disrupting operations. Attacks within this domain can be made by any individual, organization, or state-sponsored group with the intent to disrupt or stop operations by the exploitation of backdoors or by the use of viruses, bots, and so on.

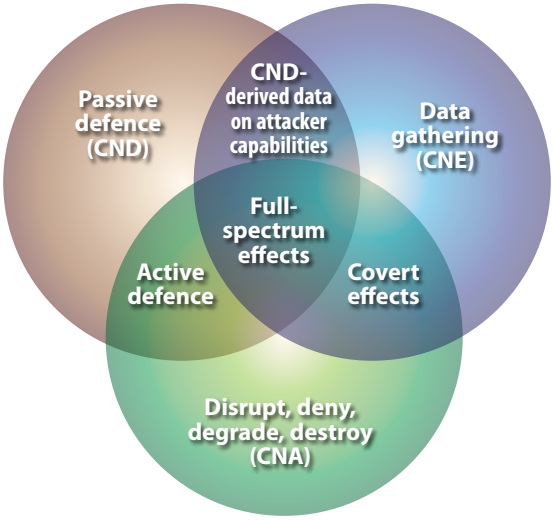

Figure 2-3. Interdependencies Between Computer Network Operations Disciplines[5]

The RCAF has attempted to provide secure networks with systems and measures built in to deal with attacks against the information domain. These systems and measures consist of backups, virus protection, user procedures, and various other protocols. This, however, will not guarantee a secure operating environment. "Once a threat is detected or suspected then some or all of the following actions can be taken:

a. physically unplugging the target device;

b. blocking related traffic using a firewall;

c. redirecting the attacker into a 'honey pot'[6] to observe their techniques and intent; and

d. conducting CNA to disable the attacker.

"The recovery process if required may include:

e. restoring a device from a known clean backup image;

f. decontaminating one or more hosts from a virus infection; and

5 DND, Defence Research and Development Canada – Centre for Operational Research and Analysis, DRDC CORA TM 2009-058, *CF Cyber Operations in the Future Cyber Environment Concept*, DRDC, December 2009, 8 (hereafter cited as DRDC CORA TM 2009-058).

6 "In computer terminology, a **honeypot** is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers." WIKIPEDIA, http://en.wikipedia.org/wiki/Honeypot_(computing) (accessed July 20, 2011).

g. investigating possible changes to prevent a second occurrence of the attack. This might correspond to the Sense domain's 'battle damage assessment,' which may be an intelligence activity."[7]

A component of defending against threats is educating the users about the role that they play in the security of the network, and the potential real effect of disregarding security procedures. It only takes one user to insert an infected universal serial bus (USB) drive into an inside host to introduce a backdoor into the network for the enemy, from which point the entire network may be vulnerable to information leakage or destruction. The informational domain can be considered as part of the greater cyber defence.

MORAL DOMAIN

Potential adversaries will look for ways to attack our will to fight using anything that falls within the moral domain. This is a very cost-effective weapon that can be exploited by adversaries who cannot match us using conventional battlefield operations. The methods of attack will and can include attacks on our homeland, attacks to provoke our forces into action of dubious purpose and/or uncertain chance of success, and attacks to undermine our legitimacy and effectiveness both in and out of theatre. These types of threats are often difficult to counter, particularly when they are frequently settled in the arena of public opinion or the media. The attacks listed below are methods used, but are not all inclusive of this domain.

a. **Psychological threats**: These threats can be demonstrated and become effective in a number of ways, primarily through the use of the media. This includes messages which are given out by the military through its public affairs personnel. These messages are relayed to personnel both at home and abroad or deployed, by the media, and by military and civilian journalists. If the public at home is not given the right message, their support of the mission and deployed personnel will waiver and fall (see Figure 2-4), possibly causing significant ethical dilemmas by mission personnel.

b. **Morale and cohesion of the unit**: This can have a devastating effect on the operation/task if due consideration is not given to this facet of Shield. If morale and unit cohesion are not maintained, effectiveness of the unit and the ability to implement and maintain the Shield function will be greatly damaged.

7 DCDR CORA TM 2009-058, 20.

Figure 2-4. War Protest Toronto 2008[8]

c. **Attacks against the homeland**: Deployed personnel need to know that their family and friends are safe and protected. If personnel are not assured of this, their focus will not be on the mission.

d. **Maintaining mission legitimacy**: Personnel need to feel confident in the legitimacy of their mission. There is the need for international organizations to validate their actions, such as the United Nations (UN), the North Atlantic Treaty Organization (NATO), etc.

e. **Rules of engagement**: These need to be clear, concise, and valid, leaving no question as to what actions are acceptable and available. A thorough understanding of ROE is needed to mitigate any moral dilemmas.

8 Miles Storey, "What Is It Good For?," photo by *Torontoist*, 23 October 2008, http://torontoist.com/2008/10/phototo_what_is_it_good_for.php?gallery0Pic=37# (accessed July 20, 2011).

f. **Indigenous people and non-military threats**: These include hostile activities from civilian populations, criminals, and insiders. An insider may be a member of the CF, a Canadian civilian or employee of the DND, a Canadian contractor, a locally-employed civilian (LEC) of the host nation (HN), or an employee or contractor who is neither a Canadian nor a citizen of the HN (a third-country national) who has access to RCAF assets. These threats may be unorganized or well orchestrated and may take the form of compromised information, demonstrations, occupied facilities, riots, physical assaults, or kidnappings. Insiders may threaten RCAF interests by disclosing sensitive or classified information, making decisions that favour dissident groups, or by assisting asymmetrical attacks. Criminal activity may be a sign of future actions or may provide advanced indications and warning of attack.

CAPABILITIES OF SHIELD

"The Shield function is part of a system that is designed to deter, prevent and pre-empt hazards before they pose a risk, and to detect, deflect or otherwise counteract the direction of potential attacks on critical weak points using active, integrated and layered responses. The Shield function operates within a framework designed to provide agile, precise and scalable protection across the complete spectrum of [Royal Canadian] Air Force activities. This is no more apparent than in the [North American Aerospace Defence Command] NORAD program which includes many of the aspects of the Shield function (in concert with several other functions).

Figure 2-5. Capabilities of Shield

"It does this through the understanding and application of all the Shield function domains (physical, informational and moral) through a systematic assessment of activities considering and applying to the following actions:

a. **pre-emptive**: take action in an effort to disrupt, interdict or destroy an adversary's ability to conduct actions against friendly capabilities, systems or platforms;

b. **detection**: monitor and track an adversary's actions and movements through SA and provide decision makers with understanding of who the adversary is;

c. **assessment**: evaluate all hazards to the deployed force and allow decision makers to refocus detection and identification capabilities or refine understanding and predict adversarial intent;

d. **warning**: issue indicators and warnings to decision makers from various levels of government, industry and the public. The use of predictive tools will provide the ability to sense and direct response to all hazards and provide protection to critical systems;

e. **defence**: defend forces using active and passive measures using both kinetic and non-kinetic means. Passive measures provide a preventative and deterrent effect. Active measures employ kinetic and non-kinetic actions to disrupt and interdict an adversary while continuing to protect deployed forces and multinational partners; and

f. **recovery**: absorb a hazard, achieve continuity and resume operating functions in minimum time, even in the face of sustaining losses or damage."[9]

These Shield function capabilities must be considered, integrated, planned for, and if required, mitigated when planning operations and missions. As an example, the Act function must consider some or all of these when planning a Shape mission that will require overhead air protection against a large number of factors, such as ground to air missiles, electronic warfare, and the like. The Act function needs to plan for adequate countermeasures to any and all negative effects that can affect the operation or mission. This applies equally to all other functions. These negative effects and adverse factors can be countered and mitigated using the risk assessment and mitigation process.

A vulnerability and risk-based, analytical approach will manage the effects of all hazards within the entire Shield function and provide the necessary focus on formulating the most appropriate course of action in all domains.

9 DRDC CORA TM 2009-005, 10–11.

As part of the Shield function, protection will be distributed and consist of overlapping capabilities and redundancy of systems, with a subsequent requirement for a dynamic risk assessment process, and analytical tools to support re-prioritization of resources. This vulnerability and risk-based analysis demands closer synchronization and linkages between detection, identification, and warning systems (i.e., the Sense function), and the risk analysis process (i.e., the Shield function), in order to mitigate national vulnerabilities.

Central to the Shield function is a much broader and deeper requirement for information sharing. A clear recognition of the linkages and capabilities among the various functions is imperative for Shield activities. The Shield function should be able to minimize the reliance on protection solely through mass defences and firepower by expanding on the requirement for improved SA. The application of key principles, agility, and precision will assist in mitigating the vulnerabilities within the Shield function. "Some of the improved capabilities expected to result from this application include the ability to

a. converge and adjust activities, expertise and resources in a more timely manner;

b. achieve timely and anticipatory responses to emerging threats;

c. match, adapt and precisely tailor all Shield functions to a wide range of mission requirements;

d. seamlessly integrate, coordinate and connect other departments (as required) and security partners to achieve desired effects;

e. capitalize on multiple inter-dependencies of critical infrastructure;

f. facilitate a convergence of physical, informational and moral capabilities;

g. synchronize the Shield function with Act, Sense and Command at all levels;

h. sense and direct responses to threats and the protection of critical systems; and

i. provide a robust, scalable and comprehensive Shield function for complex operating environments."[10]

10 DRDC CORA TM 2009-005, 12.

INTERDEPENDENCY OF SHIELD WITHIN OTHER FUNCTIONS

The Shield function is both an enabler for and is reliant upon Sense, Command, Act, Generate, and Sustain functions to be effective. As such, Shield has a number of interdependencies with these other functions.

In many instances, the capabilities of one function cannot be carried out without the capabilities of another function being in place. Some of these interdependencies require the activities of the Shield function to be considered, mitigated, planned for, and implemented in order to accomplish the commander's intended objective. Furthermore, the activities of the other functions must be able to work in unison with elements of Shield to provide the commander with the full complement of activities required to carry out the mission.

a. **Shield and Command**: As with the other functions, the Command function must be fully integrated. The Shield function will rely heavily on the Command function for direction during initial setup and as the operational situation changes. Once Sense and Shield functions have provided the pertinent information to the commander, Shield will rely on the Command function for speedy and appropriate direction. This direction will be used by the Shield function to eliminate, mitigate, or move the threat or risk. The Command function relies on Shield to be able to perform its duties in a reasonably safe environment, thereby allowing it to execute its Sustain, Act, Generate, and Sense functions.

b. **Shield and Sense**: When considering the Shield function, commanders require the Sense function to provide them with information on both red and blue force capabilities and intentions on a sustained basis. This information allows the Shield function to eliminate, mitigate, or move the threat or risk identified as the situation demands. This provides the other functions, including Sense, a relatively safe and stable location from which they can carry out their mission or operation. The Shield function will rely on the Sense function for the capability of anticipating, detecting, identifying, warning, and tracking the full range of threats. Detection and warning must be carried out with sufficient speed and precision to allow for the Risk Assessment Analysis process to be undertaken. This will give the Command function options for the appropriate defensive and/or countermeasures to be taken; for example, a Sea King helicopter may be dispatched to carry out a Shield function (physical domain FP) and Sense mission simultaneously in support of its ship or the naval task group to which it belongs. It also can be redirected to provide Shield

function (physical domain "top cover") and Shape at the same time, protecting the naval task group by launching weapons in support of either the Shield or Shape function.

c. **Shield and Act**: The Shield function will need to be considered together in both of the Act functions (Shape and Move). A flight of six fighter bombers may be dispatched to do a Shape function in support of an operation. During this operation, several of the fighter bombers may be designated as escort to provide a Shield function over the remaining aircraft engaged in the Shape function. The Act function needs to consider this Shield function activity and others similar to it by eliminating, mitigating, or moving the threat or risk when carrying out its mission or operational planning process. The RCAF may be required to provide a Shield function (overhead cover or covering fire) in support of Canadian Army Act and Manoeuvre operations or during engagements with opposition forces. This overhead protection could be considered a Shield function. Shape function support can be requested by FP forces, and this type of Shape function in support of the Shield function activity (physical domain FP) can be requested for FP elements engaged outside the camp wire but within the air component commander's (ACC) area of responsibility (AOR), which may extend 15 to 20 kilometres outside the camp perimeter. The Move function may also be required to provide fresh troops and air personnel to replace outgoing FP units supporting the Shield function.

d. **Shield and Sustain**: Sustain is one of the main functions that requires the Shield function as an umbrella to carry out its activities. Shield provides an environment in which Sustain function can operate, both within the camp/airfield and during sustainment operations, including those that involve forward operating locations (FOLs) and ground resupply missions. The ACC will be required to consider all risks and threats identified by the Shield function, and to eliminate, mitigate, or move them in order to carry out the Sustain function, such as (a logistical convoy) supplying an FOL or forward operating base (FOB), during which air cover (a Shield function under Act) may be required. Shield requirements may also include the sustainment of OGDs as well as supporting humanitarian operations and domestic operations, such as floods and ice storms. The Sustain function is also necessary to support the Shield function (physical domain FP effort) with equipment and resupply, especially replacing expended materiel and damaged or worn equipment and parts.

e. **Shield and Generate**: "Generate develops and prepares an aerospace force to meet force employment requirements…. Generating forces to provide aerospace power is an ongoing activity that involves three main elements: developing required force capabilities, conducting force readiness activities, and establishing programs to prevent the accidental loss or degradation of these capabilities."[11] The Shield function provides the safest possible environment with which the Generate function can conduct its activities. Essential to the Generate function are the measures which are put in place to shield or prevent any loss or degradation to RCAF capabilities. Generating and employing air force assets involves a certain degree of risk, which may result in death, serious injury, loss of equipment, degradation of capability, or damage to the environment. Organizational loss prevention programs are therefore incorporated early in the life cycle of any weapon system or other materiel, from introduction through to its employment, sustainment, and ultimately, during its disposal. The main programs shielding RCAF losses and damages are the Flight and General Safety Programs, the Airworthiness Program, and the Environmental Stewardship Program.

All functions—Command, Sense, Act (Move and Shape), Sustain, and Generate—have unique interdependencies and ramifications when dealing with the Shield function. Since the Shield function is more of a mindset rather than a specific group of RCAF personnel assigned to the Shield function, the individual functions will outline and describe their relationship with Shield in more depth within their individual function and subordinate doctrine manuals.

SUMMARY

This chapter introduced the three main components of the Shield function: physical domain, informational domain, and the moral domain. It described the various facets of each domain, and how each domain can affect RCAF operations. It explained the capability of the domains and how each should be considered / dealt with during the application of the Shield function, through pre-emptive action, detection, assessment, warning, defence, and recovery. Finally, it explained the relationship and interdependencies with the other functions. It directed to each of the component functions' keystone doctrine documents for more specific guidance with regards to the individual relationship within the Shield function.

11 B-GA-400-000/FP-000, *Canadian Forces Aerospace Doctrine,* 2nd ed., December 2010, 49, http://trenton.mil.ca/lodger/CFAWC/CDD/Doctrine/Pubs/Strategic/B-GA-400/Edition_2/B-GA-400-000-FP-000-Edition_2.pdf (accessed July 13, 2011).

CHAPTER 3

APPLICATION OF THE SHIELD FUNCTION

CF Photo: Cpl Owan Budge

INTRODUCTION

The fundamental aim of the Shield function is to enhance operational capabilities and mission assurance, with minimal loss due to threats and risks. It does this through the process of risk management. The risk areas considered that relate to Shield are those risks that have consequences across the physical domain, informational domain, and moral domain.

MECHANICS OF SHIELD

RESIDUAL RISK

"Although traditional military threats will not disappear for [the CF] in the foreseeable future, non-conventional threats attempting to exploit weaknesses and undermine strengths appear to be the most likely method of attack. Accidents and the environment also pose threats to our forces. As the [RCAF] will often operate in areas that feature unhealthy environmental conditions and rudimentary or damaged infrastructure (including airfields, roads, sanitation and public health services), measures will be required to protect personnel from endemic diseases, natural disasters, accidents, and the accidental or intentional release of toxic industrial [chemicals, biohazards, radioactive materials, toxic industrial] materials (TIMs), or other [threats]." [1]

Royal Canadian Air Force operations, and hence the Shield function, "are inherently complex, dynamic, dangerous, and involve the acceptance of risk. The level of risk is often related to potential gain [or loss], so leaders must be able to weigh the estimated cost properly against the desired ends for each operation. The commander's judgment balances the requirement for mission success with the inherent risks. Leaders have always practiced risk management in military decision making; however, the approach to risk management and degree of success vary widely depending on the leader's level of training and experience. The CF operational planning process (OPP) is a methodology that is already designed to identify and manage risk to a certain degree by examining each situation and enabling the commander to choose a course of action that is most likely to produce mission success. When risk management is integrated into OPP, this process ensures that all risks are adequately examined, measures are put in place to mitigate them to an acceptable level, and residual risks are fully understood."[2]

Risk and threat levels are determined in relationship to the value of an asset, and its mission criticality if it was or was not available. This is why

1 B-GA-405-001/FP-001, Aerospace Force Protection Doctrine, August 2008, 1–6, http://trenton.mil.ca/lodger/CFAWC/CDD/Doctrine/Pubs/Operational/405_Series/B-GA-405-001-FP-001.pdf (accessed January 12, 2012).

2 B-GJ-005-502/FP-000, *Joint Doctrine Manual-Risk Management for CF Operations,* November 2007, 103.3., http://www.cfd-cdf.forces.gc.ca/cfwc-cgfc/Index/JD/Pub_Eng/J5%20Publications/CF%20Joint%20Doctrine%20-%20B-GJ-005-502%20FP-000%20-%20Risk%20Management%20for%20CF%20Operation-%20EN.pdf (accessed July 13, 2011).

risk modeling and analysis dictate the requirement to conduct criticality assessments of assets, threat assessments, and vulnerability assessments to understand the total risk exposure level.

In the Shield function, risk includes any element that undermines or negatively impacts the ability to protect tangible and intangible elements, including those elements that invariably affect public support. It should be pointed out that risk in this context does not mean the operational risk of failure inherent in conducting any particular mission. Nor does it refer to the threats that the Shield function is required to detect, mitigate, and defend against.

CF Photo: Cpl Shilo Adamson

CONTINUOUS SHIELD APPLICATION

Commanders should realize, however, that some factors in the residual risk equation cannot be quantified and stem from the mere act of carrying out operational and tactical missions as much as from science. There is expectation that all RCAF personnel will conduct due diligence in reporting any offensive and/or defensive activities that may deter, detect, pre-empt, mitigate, or negate the commander's intentions, and/or any threats against the RCAF's aerospace operations and assets.

The Shield function needs to be based more on risk management than risk elimination. It is not possible to develop a Shield function capability for every scenario, covering all the various possible factors, pieces of equipment, and operations. The management of risk should be aimed at the mitigation of as many of the factors as possible, focusing on the

mission-critical elements. One of the goals of Shield is to minimize the risks to a manageable level so that the Command element is capable of carrying out its operation or mission. This can be accomplished by the continual process defined in Figure 3-1.

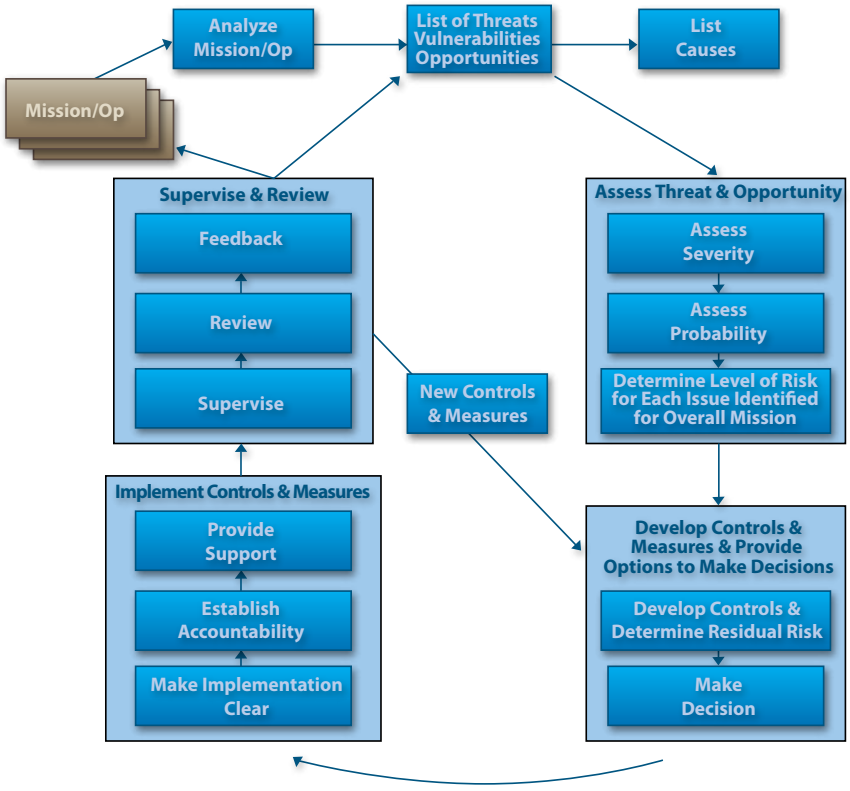

Figure 3-1. Continuous Application of the Shield Function[3]

This continuous application of the Shield function is required when generating, training, deploying, and employing any RCAF element. Generating, deploying, and employing RCAF assets highlight the necessity to balance risk against resource constraints when carrying out the Shield function.

"Some measure of risk is inherent in all military operations. By its very nature, the application of force will place individuals and resources in harm's way. Many mechanisms already exist to assist in the control and mitigation of risk. They include doctrine, standard operating procedures (SOP), drills and technical design standards. A clear process of risk management is required in military planning to ensure that threats are

3 Adapted from B-GJ-005-502/FP-000, Joint Doctrine Manual, *Risk Management for CF Operations,* November 2007, http://www.cfd-cdf.forces.gc.ca/cfwc-cgfc/Index/JD/Pub_Eng/J5%20Publications/CF%20Joint%20Doctrine%20-%20B-GJ-005-502%20FP-000%20-%20Risk%20Management%20for%20CF%20Operation-%20EN.pdf (accessed July 14, 2011).

fully considered, appropriate measures taken to minimize their effects, and that risk decisions are fully understood. Risk management assists in developing the proper balance between means and ways to achieve the desired end state."[4] For more in-depth guidance in risk management, refer to B-GJ-005-502/FP-000, *CFJP Risk Management for CF Operations.*

SUMMARY

"In the end, Shield encompasses the all-inclusive actions and steps to protect the most important resource in today's battlespace—the individual [airman/airwoman]—as well as the other platforms and friendly force systems required to ensure freedom of action [and successful completion of a mission]. An absolute Shield capability spans every element of the physical and [informational and moral domains] across the entire battlespace…. [To this end], Shield must include a mix of active and passive measures to assure the best possible chance of surviving against the myriad of threats [physical, informational, and moral] likely to exist in [the present] and future battlespace. After all, to succeed and win while deployed operationally, [airmen and airwomen] must be secure in the knowledge that they are shielded by the very best individual … systems, weapons platforms, health care, support systems, and casualty evacuation systems. Additionally, they must remain firm in the belief that their cause is just, that their families and loved ones are safe, and that they have the support of their nation. In sum, the Shield function [ensures] that these complex and interrelated issues are effectively addressed."[5]

CF Photo: Cpl Marilou Villeneuve

4 Ibid., 101.1.
5 *Future Force Concepts for Future Army Capabilities*, 2003, 133.

GLOSSARY

The definitions contained in this glossary are derived from a number of sources. Where this publication is the source of a definition, no source is indicated. Definitions taken from other sources are indicated in parentheses at the end of each term, utilizing the following abbreviations:

a. B-GA-405-001 – B-GA-405-001/FP-001, *Aerospace Force Protection Doctrine, http://www.airforce.forces.gc.ca/cfawc/CDD/Doctrine/Pubs/Operational/405_Series/B-GA-405-001-FP-001.pdf*

b. B-GJ-005-314 – B-GJ-005-314/FP-000, Joint Doctrine Manual, *CF Joint Force Protection Doctrine*, http://www.cfd-cdf.forces.gc.ca/cfwc-cgfc/Index/JD/Pub_Eng/J3%20Publications/CF%20Joint%20Doctrine%20-%20B-GJ-005-314%20FP-000%20-%20CF%20FP%20Doctrine%20-%20EN.pdf

c. B-GJ-005-502 – B-GJ-005-502/FP-000, Joint Doctrine Manual, *Risk Management for CF Operations*, Change 1, http://www.cfd-cdf.forces.gc.ca/cfwc-cgfc/Index/JD/Pub_Eng/J5%20Publications/CF%20Joint%20Doctrine%20-%20B-GJ-005-502%20FP-000%20-%20Risk%20Management%20for%20CF%20Operation-%20EN.pdf

d. DTB – *Defence Terminology Bank*, http://terminology.mil.ca/term-eng.asp.

controls
Actions taken to mitigate risks normally by reducing their probability or severity.

informational domain
The sphere in which information and data reside. (DTB record 41414)

information superiority
The operational advantage derived from the ability to acquire, exploit, protect and disseminate an uninterrupted flow of information while denying an adversary's ability to do the same. (DTB record 41413)

moral domain
The sphere in which people interact on a psychological, ethical and/or cognitive level. (DTB record 41423)

physical domain
The sphere in which people live and work. (DTB record 41433)

residual risk
The risk remaining after controls have been identified, selected and implemented for the threat.(B-GJ-005-502)

risk
Chance of failure, injury or loss, expressed in terms of probability and severity of a threat agent exploiting a vulnerability. (B-GJ-005-314, modified)

risk assessment
A systematic method of identifying and evaluating hazards and/or threats, the results of which are derived from probability and severity. (DTB record 43999)

risk decision
The decision to accept or not accept the risk(s) associated with an action; made by the commander or individual responsible for performing that action.

severity
The expected consequence of an event in terms of degree of injury, property damage, or other operation or mission-impinging factors (loss of combat power, adverse publicity, etc.) that could occur.

threat
A person, group or thing with the capability or intent to adversely affect mission accomplishment. (DTB record 44002)
Note: conditions that can adversely affect the accomplishment of the mission are confidentiality, integrity or availability of assets.

LIST OF ABBREVIATIONS

ACC	air component commander
CBRN	chemical, biological, radiological and nuclear
CF	Canadian Forces
CFAWC	Canadian Forces Aerospace Warfare Centre
CFJP	Canadian Forces Joint Publication
CNA	computer network attack
CND	computer network defence
CNE	computer network exploitation
CNO	computer network operations
DND	Department of National Defence
DTB	Defence Terminology Bank
FOL	forward operating location
FP	force protection
HN	host nation
ISR	intelligence, surveillance and reconnaissance
JIMP	joint, interagency, multinational and public
NGO	non-governmental organization
OGD	other government department
Op	operation
OPP	operational planning process
PC	personal computer
RAF	Royal Air Force
RCAF	Royal Canadian Air Force
ROE	rules of engagement
SA	situational awareness

LIST OF REFERENCES

B-GA-400-000/FP-000, *Aerospace Doctrine*, 2nd Edition, December 2010, http://trenton.mil.ca/lodger/CFAWC/CDD/Doctrine/Pubs/Strategic/B-GA-400/Edition_2/B-GA-400-000-FP-000-Edition_2.pdf (accessed July14, 2011).

B-GA-405-001/FP-001, *Aerospace Force Protection Doctrine,* 8 August 2008, *http://www.airforce.forces.gc.ca/cfawc/CDD/Doctrine/Pubs/Operational/405_Series/B-GA-405-001-FP-001.pdf* (accessed July 14, 2011).

B-GJ-005-500/FP-000, *Canadian Forces Joint Publication (CFJP) 5.0 Operational Planning Process (OPP)*, Change 2, April 2008, http://dsp-psd.pwgsc.gc.ca/collection_2010/forces/D2-252-500-2008-eng.pdf (accessed July 14, 2011).

B-GJ-005-502/FP-000, Joint Doctrine Manual, *Risk Management for CF Operations,* November 2007, http://www.cfd-cdf.forces.gc.ca/cfwc-cgfc/Index/JD/Pub_Eng/J5%20Publications/CF%20Joint%20Doctrine%20-%20B-GJ-005-502%20FP-000%20-%20Risk%20Management%20for%20CF%20Operation-%20EN.pdf (accessed July 14, 2011).

DND. *Canada First Defence Strategy,* 12 March 2010, http://www.forces.gc.ca/site/pri/first-premier/defstra/summary-sommaire-eng.asp (accessed July 14, 2011).

_____. Defence Research and Development Canada - Centre for Operational Research and Analysis (DRDC - CORA). CORA TM 2009-005, *Capability Domain Concept, Shield Capability Domain*, January 2009.

_____. DRDC - CORA TM 2009-058, *CF Cyber Operations in the Future Cyber Environment Concept*, December 2009.

_____. Directorate of Land and Strategic Concepts, *Future Force Concepts for Future Army Capabilities* (Kingston, ON: 2003), 130, http://www.army.forces.gc.ca/DLCD-DCSFT/pubs/special/futureforce/FPAC_eng.pdf (accessed July 14, 2011).

Friesen, Shaye K., and Andrew N. Gale. "Slaying the Dragon: Future Security Environment & Limitations of Industrial Age Security." *Canadian Military Journal* 11, no. 1. http://www.journal.dnd.ca/vo11/no1/07-friesen%20gale-eng.asp (accessed July 14, 2011).

Gizewski, Peter, Michael Rostek, and Andrew Leslie. "Comprehensive Operations: Moving to a JIMP-capable Land Force." *Vanguard* (2006), http://www.vanguardcanada.com/ComprehensiveOperationsGizewskiRostekLeslie (accessed July 14, 2011).

R. J. Hillier. Director Land Strategic Concepts. DLSC 2007-04-27, *Omni-Dimensional Shield in Future Conflicts* (Ottawa: DND).

CF Photo: Cpl Shilo Adamson