NATO
OTAN

NATO SPECIAL OPERATIONS HEADQUARTERS

Comprehensive Defence Handbook

Volume I

Edition A Version 1
December 2020

Intentionally blank

Foreword – COM NSHQ

Enabling Comprehensive Defence is a key component of our AJP 3.5 Military Assistance mission's Force Multiplier Special Operations Forces (FMSOF) expertise. While countries may be in different stages of developing these comprehensive defence capabilities, all will benefit from enhancing and synchronizing deterrent and comprehensive defence networks and tools. Our intent is for this purely defensive handbook to assist all NATO and Partner countries that seek to optimize their country's deterrence and comprehensive defence capabilities.

Comprehensive defence is not limited to SOF, military or government practitioners. Rather, it centres on enabling an entire country through a whole-of-society, whole-of-country deterrent and defensive approach. This handbook therefore focuses on roles and functions of society, groups and government entities working together to improve deterrence and defence of their homeland. The pillars of comprehensive deterrence and defence activities across phases of preparation, response and recovery provide a framework for practical checklists and implementation principles.

The aim of this this handbook and the checklists contained within it is to practically assist in the development of a national programme designed to enable all members of society to contribute to comprehensive deterrence and defence. Use of the handbook will foster a shared understanding that underscores increased coordination and synergized effects. This handbook is a key tool for trainers to leverage within their own countries as they develop the comprehensive deterrent and defence capabilities for their country. While readers may find significant benefit in this first edition of the comprehensive defence handbook, I welcome your feedback so that we can improve this handbook as we republish updated versions of yearly. Your additional considerations, best-practices and recommendations will also be helpful as we update data in our comprehensive defence courses, seminars and table-top exercises.

Comprehensive Defence is enshrined in the defensive resilience and resistance principles of Article 3. This handbook and the techniques within are purely defensive in nature, and will assist in the development truly comprehensive deterrence and defensive networks.

Sincerely,

Eric P. Wendt
Lieutenant General, USA Army
Commander

Intentionally blank

NATO SPECIAL OPERATIONS HEADQUARTERS

QUARTIER GÉNÉRAL
DES OPÉRATIONS SPÉCIALES DE L'OTAN

RUE CLARK, BLDG 915
7010 SHAPE, BELGIUM

File Ref:	NSHQJ9/IBG	**Tel:**	+32 (0)65 44 7111
		Tel:	+32 (0)65 44 + ext
Date:	1 December 2020	**Email:**	nshqregistry@nshq.nato.int

NSHQ PUBLICATION

COMPREHENSIVE DEFENCE HANDBOOK

Status. This is an original NATO Special Operations Headquarters (NSHQ) publication.

1. **Purpose.** To provide fundamental concepts and principles for countries to develop, enhance, or redefine their approach to Comprehensive Defence.

2. **Applicability.** Recommendations within this handbook are based upon reference publications and best practices. The guidance is meant to be informative rather than authoritative. It does not supersede existing doctrinal publications. This handbook is primarily written for countries desiring to implement or refine a comprehensive whole-of-society approach to national defence.

3. **Publication Updates.** NSHQ will review this publication at least annually and update as needed. Suggestions for updates should be directed to the proponent.

4. **Proponent.** The proponent of this publication is the NSHQ Strategy, Concepts and Experimentation Directorate.

5. **Distribution.** As required.

Eric P. Wendt
Lieutenant General, USA Army
Commander

Intentionally blank

NSHQ Change Proposal Comment Matrix

For changing, correcting, or removing current and/or inserting new content.

Comment Guidelines for the Originator:

C – Critical

S – Substantive

E – Editorial

Serial	C / S / E	Originator	Para	Sub-Para	Comment	Rationale	Adjudication (NSHQ Doctrine)
					Insert then highlight, or line out text to be modified and propose a recommended course of action. General observations without proposed solutions should not be submitted.	Rationale will be submitted for all comments	A - Approved AA - Approved as amended NA - Not Approved

Note: This table may be copied and pasted into an email to allow for more room to comment.

Submission:
Submit requests to modify publications to NSHQ Concepts Directorate, with a cover letter containing basic contact information for the originator and organization.

Intentionally blank

Table of Contents

Table of Figures

List of Tables

Intentionally Blank

Preface

Purpose. The *Comprehensive Defence Handbook* is intended to serve as a guide for implementing a whole-of-society approach to national defence. It was authored by the NATO Special Operations Headquarters (NSHQ) to highlight the critical roles Special Operations Forces (SOF) can perform in all phases of Comprehensive Defence. However, it also recognises that SOF is a relatively small component of an effectively integrated national defence and security apparatus. Thus, whether applied by a private individual, corporation, or government official, the handbook, and specifically the checklists within it, are intended to provide specific actions that can be taken by all members of society to prevent, prepare for, respond to and recover from threats to the nation's stability and sovereignty.

Relevance. Over the past decade in particular, national security professionals and scholars have duly noted the dynamic nature of the international security environment. The contemporary discourse is framed by such concepts as "countering hybrid threats (CHT)", "peer threat competition", "total defence", "resistance", and "resilience". In this context, a nation's ability to successfully deter or defend against modern threats is contingent upon its willingness to integrate all of its elements of national power, to include the power of individual citizens. To that end, rather than entering into the ongoing academic debate, this handbook presents methods for applying concepts at all levels-tactical through strategic. It also underlines SOF's unique contributions, especially its role as a catalyst, oft times helpful in facilitating whole-of-society integration. These are essential points to emphasize, given SOF's unique capabilities in terms of Comprehensive Defence. Finally, though the handbook focuses primarily on deterrence and defence against malicious acts, it does so with a clear acknowledgement that Comprehensive Defence is equally applicable to threats originating from natural or accidental causes as well.

Applicability. This handbook is applicable to any nation that seeks to implement a whole-of-society defence that is consistent with international law and accepted norms. Accordingly, it does not seek to operationalize any one nation's concepts or doctrine, nor that of any international organization. Further, by focusing on the array of recognized potential threats and challenges to any sovereign nation, the checklists contained in this handbook are useful for deterring or responding to any malicious actor, state and nonstate alike. *Comprehensive Defence,* as presented here, is certainly applicable when preparing for, responding to or recovering from natural and accidental events that may significantly threaten a nation. However, as a NATO SOF handbook, it understandably concentrates on the security dimension of Comprehensive Defence.

Handbook Organization. This handbook is divided into two Volumes. Volume I presents considerations for government officials to take into account when enabling members of the public to participate in comprehensive defence. Volume II is a template, which, when tailored to a nation's needs, can be used to inform the average member of society of ways they can contribute to comprehensive defence. Taken together, Volumes I and II provide a coherent set of tools and checklists to guide a nation's implementation of Comprehensive Defence.

Intentionally Blank

Introduction – Framework and Supporting Concepts

Section 1 – Introduction

I. **Definition.** For the purpose of this handbook, *Comprehensive Defence is defined as* ***an official Government strategy, which encompasses a whole-of-society approach to protecting the nation against potential threats***.

II. **Scope.** Volume I of the handbook is designed to guide the public sector's role in leading the design, implementation and execution of Comprehensive Defence in accordance with the definition above. It seeks to distil relevant concepts and best practices into a practical framework and easy to follow checklists.

III. **Context**. Throughout, the handbook considers Comprehensive Defence in terms of 21st century security challenges. It addresses events that would significantly threaten a nation's peace, security and way of life. Such events may be generated by states, non-state actors, natural phenomena or major accidents.

IV. **Actors**. Unlike traditional responses, which concentrate on government actions, society forms the bedrock of Comprehensive Defence. The actors, comprising the "whole-of-society" can be considered in three categories (table 0-1).

a. Figuratively speaking, the public sector only comprises 2% of the nation's prevention and response capability. This means that the majority of the population is contained in the two non-governmental categories, the private and civic sectors, sometimes referred to as "the 98%".

b. A key Comprehensive Defence objective is to harness the untapped capacity of "the 98%" by developing the capability and willingness of all members of society to directly contribute to their own safety, security and natural right to self-determination.

Table 1.1 Sectors of Society

COMPREHENSIVE DEFENCE ACTORS			
Public Sector		Private Sector	Civic Sector
Military	Civil		
Conventional Forces Special Forces Reserve/Home Guard	Government Ministries Emergency Management Etc.	Business Industry Privately Owned Energy Privately Owned Hospitals Other Infrastructure	NGO's Clubs Faith Groups Civic Groups Individual citizens

Section 2 – Setting the Conditions for Comprehensive Defence

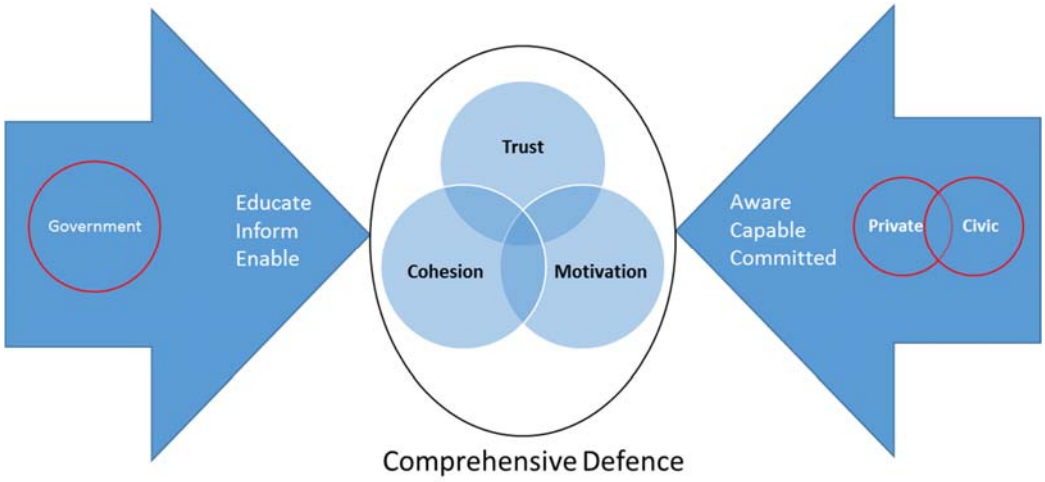


Figure 1.1 Comprehensive Defence Environment

V. Comprehensive defence requires trust, cohesion and motivation across the whole-of-society, which each sector performs a role in creating.

a. Public sector role

- Ensure agencies are able to effectively interoperate in the event of a crisis.
  - o Barriers to interagency cooperation and collaboration undermine comprehensive defence
    - Examples of barriers include legal restrictions that prohibit sharing information or resources; technical impediments (e.g., lack of interoperable communications equipment); procedural impediments (e.g., lack of interoperable tactics, techniques and procedures), etc.

- Provide the public with the tools needed to contribute to comprehensive defence
  - o Educate
    - Understanding of the nation's approach to comprehensive defence
    - Understanding of potential external threats, natural disasters and accidental events
    - Know how to contribute to help prevent, prepare for, respond to and recover from threatening events
  - o Inform. Provide up to date, accurate information on the status of potential threats and the nation's ability to respond to them
  - o Enable. Implement policies and actions that support private and civic sector participation in comprehensive defence

b. Private and civic sector role
- Aware. Stay up to date on conditions that may impact the nation's defences
- Capable. Through education and training, build the skills necessary to contribute to comprehensive defence
- Committed. Actively participate in prevention, preparation, responses to and recovery from natural, accidental and malicious events.

Section 3 – Comprehensive Defence Framework

VI. Figure 1.2 provides a graphical depiction of the Comprehensive Defence Framework, which is explained below.

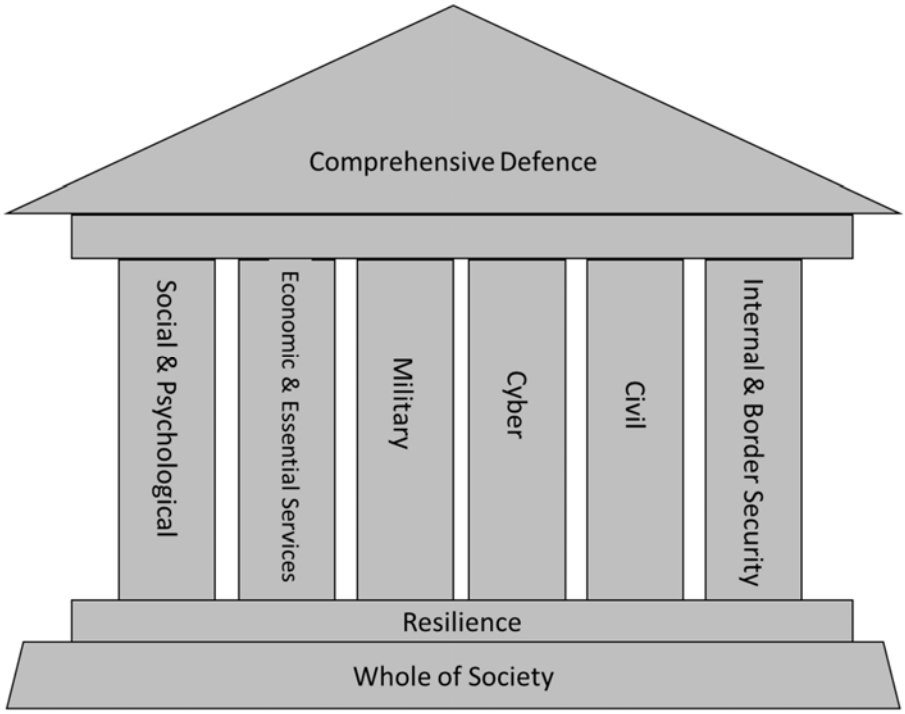


Figure 1.2 Comprehensive Defence Pillars

VII. **Resilience**. Resilience is the foundation atop the whole-of-society bedrock. It is defined as "*the will and ability to withstand external pressures and influences and/or recover from the effects of those pressures or influences*"[1] in an individual and collective manner. Resilience is built through **civil preparedness** and is achieved by continually preparing for, mitigating and adapting to potential risks well before a crisis. Once achieved, it needs to be habitually nurtured. Even when responding to crises, a concerted effort must be placed on sustaining resilience, as it must be maintained no matter how long a crisis situation may last. Any

[1] Resistance Operating Concept (ROC).

factors that erode resilience must be resolved immediately, or certainly as soon as the crisis conditions allow. While balance is necessary and resource limitations are real, it is safe to assume that no aspect of a Comprehensive Defence framework can ever be "resilient enough." Complacency is the antithesis of resilience.

VIII. **Pillars**. The pillars of Comprehensive Defence are helpful in understanding the functions and actions needed to prevent, respond to and recover from crises. They are described as follows:

a. **Social and Psychological Defence** builds on the qualities of resilience and determination by reinforcing national pride and identity amongst all citizens and residents to overcome any crisis. This function also accounts for building bonds of harmony and reinforcing national integration across an oftentimes diverse population. This is accomplished by better understanding and appreciating the heritage, culture and practices of fellow members of society, thus strengthening national cohesion. The desired condition is a mentally prepared and resilient population that is well informed, has confidence in the national authorities and demonstrates the collective will and commitment to defend the country. Social and Psychological Defence also accounts for a nation's ability to communicate factual and accurate information and counter malign messaging.

b. **Economic & Essential Services** encompasses building and sustaining a strong economy and durable critical infrastructure that can sustain the nation through economic challenges and national emergencies, to include providing essential services to the population; i.e., food, water, medical support, etc. On an individual basis, one can play a part by retraining and upgrading in order to remain employable in a globally competitive economy. Government and businesses also need to prepare contingency measures to protect critical infrastructure, the economy and to maintain vital economic services during a crisis, to help ensure a resilient national population. Additional components of economic and essential services include energy, communications, transportation, critical manufacturing, and commercial facilities and financial services.

c. **Military Defence** is the mandate of the Armed Forces and the responsibility of service members, guided by civilian defence officials, to deter and counter aggression. In some nations military defence includes provisions for civic support to the military, as well as programmes and designated forces established to actively resist in the event of foreign occupation. It is recognized that military defence is becoming increasingly dependent upon the civilian infrastructures[2]. Additionally, in some nations, the military is used heavily for civil purposes, such as natural disaster relief, emergency maintenance of civil order as well as border and maritime defence.

[2] 90% of military transport is accomplished using civilian assets, over 50% of satellite communications used for defence purposes are provided by the commercial sector, 75% of host nation support to NATO operations is sourced from local commercial sources" https://www.cimic-coe.org/resources/fact-sheets/resilience-through-civil-preparedness.pdf

d. **Cyber Defence** focuses on preventing, detecting and providing timely responses to attacks or threats to critical digital infrastructure and information, while ensuring the nation has freedom of manoeuvre required to conduct and support all other Comprehensive Defence functions.

e. **Civil Defence** focuses on safeguarding all aspects of civilian life from malicious attacks and natural disasters. It accounts for crisis management, emergency management, emergency preparedness, and civil protection, with a particular concentration on emergency operations (prevention, mitigation, preparation, response, recovery). Civil Defence entails the commitment of a wide range of national resources and capabilities, to include voluntary paramilitary organizations. For example, because Civil Defence is so broadly encompassing and naturally lends itself to civic participation, a number of countries maintain national Civil Defence Corps, designed to assist the government during civil emergencies, such as flood, earthquake, invasion, or civil disorder.

f. **Internal and Border Security** are core functions for any comprehensive defence. Internal security includes public safety and law enforcement roles, as well as domestic intelligence, which is often within the Ministry of Interior or the national police force. Internal security is closely tied to civil defence, which entails emergency and crisis management and first responder rescue services. Border security is closely linked to internal security as well as maritime security close to shore and river systems. National Border Guards and Coast Guards are also often within the Ministry of Interior.

Section 4 – Phases of Comprehensive Defence

IX. Comprehensive defence is planned and executed according to three phases:

a. **Preparation.** During this phase, the nation establishes and maintains the conditions that allow for resilience. The phase is continuous, as the nation ensures all technical and human components of society have the unceasing “will and ability to withstand external pressures and influences and/or recover from the effects of those pressures or influences.” Along with reducing the tendency for accidents to occur, resilience through integrated whole-of-society preparedness serves as a strong deterrent to malicious acts that may be contemplated by a potential adversary. In short, resilience is the first line of defence against all potentially threatening events.

b. **Response.** Based on indications and warnings (I&W), and sometimes only “weak signals” when confronted with malicious hybrid activity, a nation’s response(s) may begin before or after a threat has presented itself. Responses may range from consequence management to information campaigns to armed or unarmed resistance.

c. **Recovery.** After the threat has been addressed, the nation takes the steps necessary to re-establish the conditions that existed prior to the crises. The post-crisis conditions may differ from pre-crisis situation, insofar as lessons and best practices will be incorporated into the new state of affairs.

Section 5- Related Terms and Concepts

X. While this handbook does not advocate any particular concept, there are several evolving security-related paradigms that are referenced throughout the document for context. Each is briefly introduced below.

a. **Deterrence**. "The act of persuading an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks."[3]

b. **Preparedness.** Preparedness is a key and inherent component to resilience. From the Military Defence perspective, preparedness includes the idea of readiness; i.e., the armed forces are organised, trained and equipped to deter and respond to threats to national security. However, preparedness in context of Comprehensive Defence entails more than military readiness. It also demands civil preparedness that underpins a society's ability to withstand, respond to, and recover from shocks. Achieving military and civil preparedness in this sense requires close collaboration across all sectors of society.

c. **Hybrid Warfare**. There are a variety of terms used to refer to the hybrid warfare concept: hybrid war, hybrid threats or hybrid adversary (as well as non-linear war, non-traditional war or special war). Western military bodies tend to speak in terms of hybrid threats or hybrid strategies, while academic literature speaks of a hybrid warfare. In most cases, the terms are interchangeable.
- All definitions describe a set of intentionally ambiguous activities that an adversary employs to influence an opposing nation while avoiding attribution or retribution.
- The activities may be kinetic or non-kinetic, diplomatic, informational, military or economic actions. In nearly all instances, the adversary's actions lie outside the accepted norms of international relations, if not blatant violations of international law.

d. **SOF's role in Peacetime Competition, Crisis and Conflict** is being studied across the defence and security community through the dual lenses of great power competition and hybrid warfare. The emerging concept focuses on SOF's role enhancing resilience, contributing to deterrence and preparing or incorporating asymmetric approaches into defensive *modus operandi*. The concept recognises that SOF expand the menu of options for the use of military and non-military instruments of power that may be creatively applied in any context. These activities are characterised by precision, discretion and well-mitigated risk. Effects are, therefore, based on proper employment as determined by policy makers. SOF also offer significant economy of force and reward relative to other instruments, to include an alternative when conventional military forces may be inappropriate or escalatory. Two key principles apply:
- Early employment in competition and crisis is essential for SOF success in crisis or conflict
- SOF may be employed primarily where other military or civilian assets are unable to singularly create desired effects

[3] Mearsheimer, John J. *Conventional Deterrence.* Ithaca, Cornell University Press, 1983.

Chapter 1 –Volume I Introduction

The principal audience for Volume I is government officials (the so-called 2%) of nations that are either currently implementing comprehensive defence or are considering doing so. Under these circumstances, the government has two responsibilities. One, it must ensure current structures and processes accommodate a more inclusive approach to defence and security. Two, the government must enable the rest of the society (the so-called 98%) to participate in matters of security that were previously tended to solely by state officials. The two responsibilities cannot be separated or prioritised, because they are mutually supporting.

Section 1—Overview

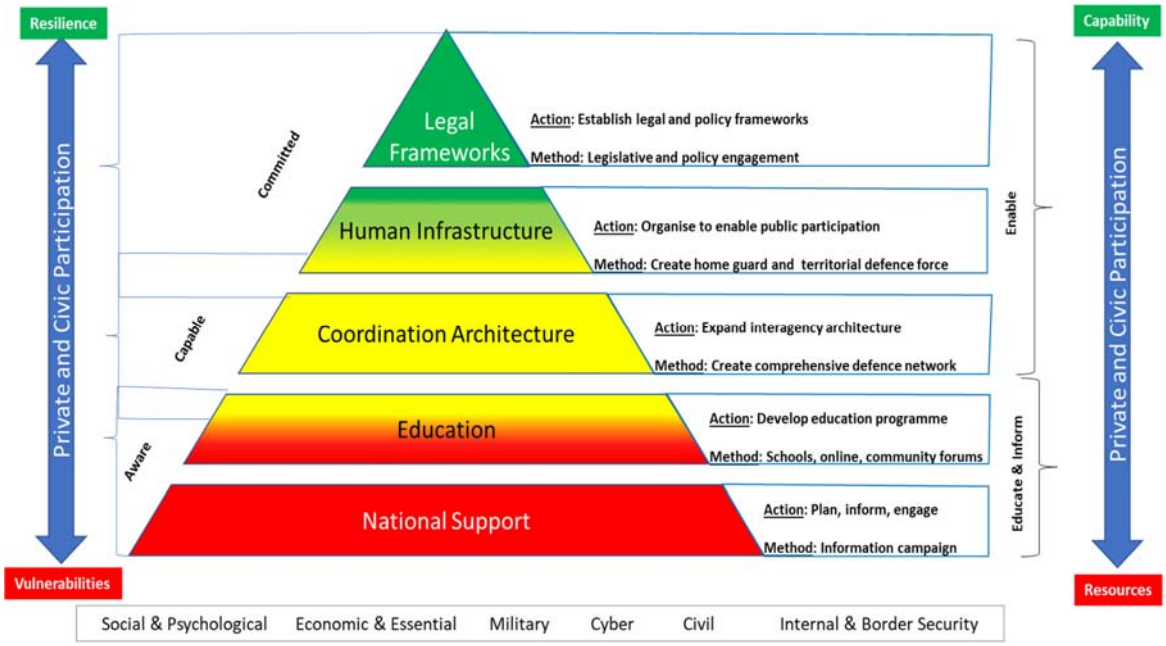


Figure 1.1 Comprehensive Defence Conditions

1.1 The considerations presented in this volume coincide with the five conditions that must be met when implementing comprehensive defence. The conditions are not phases; i.e., one condition does not need to be fully established before addressing the next. They are, however, interdependent, and some must be sustained indefinitely as integral elements of comprehensive defence.

1.2 The handbook is intended to function as a user's manual. Each chapter uses straightforward language, bullet format and highlighted boxes to recommend specific actions for the government and population to take, based on the conditions the nation aims to establish.

1.3 Volume I is designed to be used in conjunction with Volume II. Whereas the practices in this volume are most applicable to the 2%, Volume II is a tailorable template, which contains the techniques and procedures that can be applied by the 98%. There is necessary redundancy between the two volumes, though it is limited to the greatest extent possible.

1.4 It is clear throughout the volume that *this publication is designed primarily to present techniques and procedures for establishing resilience that will deter adversaries and ensure an effective defence against malicious acts*. However, it should also be clear that nearly all considerations and methods discussed within also apply to resilience and response to non-malicious events. In short, the discussions in Volume I can be easily elaborated to account for all comprehensive defence pillars.

Section 2—Organisation

1.5 The final section of this chapter contains a checklist with the key steps for implementing a whole-of-society defence. The remainder of the volume provide details in support of the checklist.

1.6 The chapters within this volume are organised according themes. The first theme, Enhancing Resilience, comprises Chapters 2 – 6.

1.7 Chapter 2 presents considerations for how the government can enable public participation in comprehensive defence by contributing to individual resilience. Chapters 3 – 5 offer approaches for describes best practices for creating a home guard and asymmetric defence component. Chapter 6 contains recommendations for designing and conducting total defence training.

1.8 With the organisational structures and training methods noted, Chapters 7 through 11 present the second theme, Deterrence and Response. Chapter 7 contains a discussion on ways to enable society to harness the deterrence value of comprehensive defence. Chapters 8 and 9 present considerations for whole-of-society defence against four types of malicious attacks. The chapters provide context for detailed discussions on the actions the population can take to prevent and respond to each of the attacks, and what the steps the government can take to enable society's actions. Chapters 10 discusses the military's role in comprehensive defence and concludes with a focus on the unique functions that Special Operations Forces (SOF) can perform. Chapter 11 closes the Deterrence and Defence theme by discussing matters of law and policy that should be accounted for when implementing comprehensive defence.

1.9 Chapters 12 through 17 are policy and process-focused and follow theme of Implementing Comprehensive Defence. The chapters include methodologies for, stakeholder mapping, gaining public concurrence, conducting assessments, and adapting defence planning processes to account for the unique aspects of comprehensive defence. Included also are detailed checklists to help with the assessment and planning process. In sum, the final

chapters look beyond malicious acts to account for all six pillars and highlight the civil preparedness aspect of comprehensive defence.

1.10 Collectively, the considerations and best practices presented in Volume I provide members of the 2% with a useful set of tools that can be applied when encouraging and enabling members of society to contribute to the nation's resilience and defence.

Table 1.1 Comprehensive Defence Checklist

Focus Area/Condition	Primary Action	Supporting Action	References
Gain Concurrence	Identify key stakeholders		
	Build concept development team		
	Develop concept to address following		
	Conduct consultations		
	Adjust concept and/or messages		
	Conduct campaign		
	Collect feedback		
Comprehensive Risk Assessment	Identify Risks		
Comprehensive Defence Plan	Develop Comprehensive Defence Framework		
Human infrastructure	Select defence force model		
	Advocate programmes to encourage volunteerism		
	Enable individual resilience		
	Enable and encourage non-volunteers		
	Establish home guard		
	Establish Asymmetric Defence Component		
Coordination architecture	Establish leadership component		
	Establish collaboration component		
Education	Establish learning groups		
	Determine subject areas		
	Build learning modules		
	Determine delivery methods		
Legal Frameworks	Interagency coordination		
	Private sector participation		
	Civic participation		
	Continuity of government		
Deterrence	Develop Strategic Narrative		
	Ensure population is familiar with strategic narrative		
	Develop communications plan		
	Associate actions with communications		
Response	Respond to malicious acts		

1.11 **Summary.** Volume I is designed to help national leaders enable their populations to contribute to a government-led, whole-of-society approach to defence, which will deter aggression and increase resilience in all areas. Although focused primarily on malicious acts, nearly all actions and recommendations brought forth in this volume apply equally hen preparing for and responding to natural and accidental events as well.

Chapter 2 Individual Resilience

This chapter provides advice and considerations for encouraging and enhancing individual resilience.

Section 1 –Overview

2.1 National resilience begins with the individual. To the greatest extent possible, every member of society should be capable of avoiding, and if necessary, caring for themselves during a crisis. Resilient individuals are also better able, and generally more willing, to contribute to whole-of-society efforts. Thus, a nation whose population is individually resilient can focus more of its resources on preventing, preparing for, responding to and rapidly recovering from crises.

2.2 This chapter offers considerations for three aspects of individual resilience
- Components
- Government encouragement and enhancement
- Education

Section 2–Components

2.3 **Individual resilience has two components**

- Psychological Resilience
  - ✓ Ability to emotionally cope with crisis and return to pre-crisis status quickly
  - ✓ Sense of national pride and belonging
- Physical Resilience
  - ✓ Individuals and families are able to care for themselves during and after a threating natural, accidental or malicious event

Section 3—Enhancing Individual Resilience

2.4 **Government role.**
- Each member of society is responsible for their own individual resilience
- However, the government should take steps, where possible, to encourage and enhance individual resilience

2.5 **Enhancing Psychological Resilience**
- Government initiatives to help enhance psychological resilience should focus on three areas
  - ✓ Education
  - ✓ Information
  - ✓ Inclusion

Table 2.1 Psychological resilience focus areas

Enabling capability or action	Reference
Educate • Programmes that provide tools required to defend oneself against disinformation, and strengthen emotional health	Vol I, Ch. 8 Vol II, Ch. 3
Inform • Programmes that ensure society is accurately informed about current conditions or trends that may affect national safety or security o Include material to guide emergency response procedures	Vol I Ch. 8, Ch. 13
Include • Programmes that reinforce common pride o Largely education and policy-based o Because they focus on addressing cultural, ethnic and ideological differences that cause discord within the society, the programmes tend to be sensitive ▪ Extremely important element of individual resilience, as social seams are commonly targeted by adversaries seeking to undermine national cohesion and influence political decision making	Vol I, Ch. 17

2.6 **Enhancing physical resilience**

- Government initiatives that contribute to physical resilience should focus on enhancing an individual's ability to avoid, identify and survive during a crisis or war (see Vol I, Ch 8 & 9 and Vol II, Ch. 3 & 4).

Table 2.2 Key Point (Enhancing Resilience)

Psychological Resilience	Physical Resilience
✓ Educate	✓ Avoid
✓ Inform	✓ Identify
✓ Include	✓ Survive

Section 4—Education

2.7 **Comprehensive defence education has two objectives**

- Enhance individual resilience
- Encourage and enable members of society to contribute to comprehensive defence

2.8 **Applicability.** Education should be designed to account for all pillars and phases of comprehensive defence. However, per the handbook's theme, this section concentrates on the security aspects of comprehensive defence education.

2.9 General Considerations

- Comprehensive defence education programmes do not mirror information programmes.
  - ✓ However, they do share many of the same characteristics (see Ch 13).
- Specific programme elements will need to be designed for each sector of society, to include the government sector, all age groups, ethnicities and sub-cultures
- Programmes will also need to evolve and adapt with changing conditions
- Comprehensive defence education is most effective when the general public is involved in designing and delivering the content
- Education programmes are not intended to simply inform decisions or encourage support, but instead to impart knowledge that stakeholders can translate into tangible skills and action.
- Education should be delivered using a range of modalities
  - ✓ Classroom
  - ✓ Online media
  - ✓ Broadcast media
  - ✓ Private enterprise
  - ✓ Civic organisations

2.10 Learning Audience

- Comprehensive defence education should be tailored to meet stakeholders' needs according to the functions they perform during each phase.
- The learning audience can be divided into four groups.

Table 2.3 Learning groups

Learning Group	Description
Group A Youth	• Focus is on social and psychological resilience
Group B Whole of society	• Foundational understanding of comprehensive defence provided to everyone
Group C Personnel from any of the entities cited in Group D below who do not perform a significant leadership function	• Builds upon foundational education received by all
Group D Personnel responsible for implementing and/or leading particular aspects of comprehensive defence	• Includes persons within and outside of the government; i.e., a combination of the 2% and 98% o National and local government o Law enforcement agencies o Public and private critical infrastructure entities o Emergency services o Home guard o Military services (Active and reserve) ▪ Special Operations Forces in particular

2.11 Learning Areas

- The tables that follow are intended to serve as references when designing the *security component* of a comprehensive defence education programme
- They are arranged according to the learning groups described in Table 2-3 (Group A, Group B, etc.)
- Group A (youth) is not addressed, but should receive age-appropriate education similar to Group B
- The education programme descriptions should not be confused with the more prescriptive training recommended for each group, which is detailed in later chapters of this volume as well as in Volume II
- Exact programme contents should be based on the outcome of the comprehensive risk assessment (Ch 15)
- Technical details, such as curriculum design, teaching modalities and harmonisation with extant educational requirements should be tailored for purpose and grounded by the advice of pedagogical experts

2.12 Group B—Whole-of-Society

- The information that would comprise this learning area should be provided to all adult members of society
- The instruction within this area will enable group members to understand the fundamentals of comprehensive defence; avoid, identify and survive malicious acts; and directly contribute to comprehensive defence if the opportunity presents itself.
- The instruction will aid in increasing whole-of-society resilience and interoperability.

Table 2.4 Whole of Society Learning Areas

Learning Block & Subject Area	Potential Modules	Reference
Social & Psychological Resilience • Explain rights and obligations as a member of society • Describe key features of national history, culture, arts, unique national geography and natural phenomenon, etc. • Apply critical thinking methods • Identify misinformation (fake news) • Apply cyber hygiene • Apply self-care, problem solving, coping skills • Explain anti-discrimination laws and policies	• Foundational laws and policies • Weaponised information • Cyber security	Vol I, Ch. 8 & 17, Sec 3
Comprehensive Defence Concepts • Describe the fundamentals of comprehensive defence	• Fundamentals of Comprehensive Defence • Resilience • Whole-of-society roles in comprehensive defence • Threat categories (natural, accidental, malicious)	
Individual Resilience	• National alert procedures	Vol II, Ch. 5

Learning Block & Subject Area	Potential Modules	Reference
• Describe national emergency alert system • Describe the purpose and contents of an Individual Resilience Kit (IRK) • Describe the actions taken to avoid and/or survive a malicious act • Describe the procedures for evacuating an emergency or disaster area	• Recognising malicious threats o Cyber o Irregular violence (terror attack) o Armed incursion • Developing and sustaining individual resilience • Survival techniques • Physical fitness	
Opportunities to contribute • Explain how to report suspicious activity or an emergency • Understand the purpose and function of a community watch organisation • Understand Home Guard structure and functions • Understand Asymmetric Defence Component structure and functions		Vol I, Ch. 4 Vol II, Ch. 5

2.13 **Group C—Direct Participants.**

- This focus area will comprise best practices, techniques and procedures for performing functions in support of whole-of-society comprehensive defence efforts, to include implementing individual resilience measures, recognising and responding to threats, defending a nation and if necessary, resisting an invading power.
- The instruction will aid collaborative planning amongst all actors in a comprehensive defence environment, cohering military, non-military and civilian/societal entities

Table 2.5 Direct Participant Learning Areas

Learning Block & Subject Areas	Potential Modules	Reference
Comprehensive Defence Concepts • Explain the Comprehensive Defence fundamental description and purpose • Describe the relationship between national resilience and Comprehensive Defence • Describe the importance of Whole of Government and Whole-of-Society approaches to Comprehensive Defence [Across all sectors including civil, private, and civic.] • Describe the relationship between comprehensive defence and deterrence	• Fundamentals of Comprehensive Defence • National defence objectives • Law and policy • Threat categories • Deterrence	Vol I, Ch 7, 9, 11
Whole-of-Society Cooperation • Explain comprehensive defence coordination architecture	• Comprehensive defence network • Home guard	Vol I, Ch. 14

Learning Block & Subject Areas	Potential Modules	Reference
• Describe the Comprehensive defence organisational structures	• Whole-of-society info sharing	
Asymmetric Defence Component (ADC) • Describe ADC structure • Explain the relationship between the asymmetric defence component, the military, the private sector and the non-volunteer component of civic society • Describe ADC training requirements and methods	• Capability integration • Principles of resistance • Resistance case studies	Vol I, Ch. 4 & 5
Employment • Describe a comprehensive defence against malicious acts	• Comprehensive defence C2 • Cyber threats • Weaponised information • Irregular violent attacks (i.e., acts of terror) • Armed incursion	Vol I, Ch. 8 & 9

2.14 **Group D Leadership Positions.**

- This focus area will comprise best practices and practical implementation of methods, strategies and procedures for whole-of-society comprehensive defence efforts, to include enhancing resilience, deterring external threats, defending a nation and, if necessary, resisting an invading power.
- The instruction within this area would provide group members the tools needed to assess and develop comprehensive defence requirements.
- The group will also learn how to design methods for teaching actors at differing levels how to apply preparedness, resilience and response measures in the relevant security environment.
- The instruction will aid collaborative planning amongst all actors in a comprehensive defence environment, cohering military, non-military and civilian/societal entities.

Table 2.6 Leadership Position Learning Areas

Learning Block & Subject Areas	Potential Modules	Reference
Comprehensive Defence Concepts • Explain the Comprehensive Defence fundamental description and purpose • Describe the relationship between national resilience and Comprehensive Defence • Outline the Comprehensive Defence pillars, phases, and assessment process • Describe the importance of Whole of Government and Whole-of-Society approaches to Comprehensive Defence [Across all sectors including civil, private, and civic.] • Describe the relationship between comprehensive defence and deterrence	• Fundamentals of Comprehensive Defence • National defence strategy • Law and policy • Threat categories • Deterrence • Stakeholder mapping • Assessment and planning	Vol I, Ch. 7, 11, 12, 15 & 16 Vol II, Ch. 2

Learning Block & Subject Areas	Potential Modules	Reference
Whole-of-Society Cooperation • Describe methods for gaining stakeholder concurrence • Explain comprehensive defence coordination architecture • Describe the Comprehensive defence organisational structures	• Comprehensive defence network • Home guard • Whole-of-society info sharing	Vol I, Ch. 3, 4 & 5 Vol II, Ch. 3 & 4
Asymmetric Defence Component • Describe ADC structure • Explain the relationship between the asymmetric defence component, the military, the private sector and the non-volunteer component of civic society • Describe ADC training requirements and methods	• Capability integration • Principles of resistance • Resistance case studies	Vol I, Ch. 4 & 5
Employment • Describe a comprehensive defence against malicious acts	• Comprehensive defence C2 • Cyber threats • Weaponised information • Irregular violent attacks (i.e., acts of terror) • Armed incursion	Vol I, Ch. 8 & 9

Table 2.7 Key Take Aways--Individual Resilience

- **Reduce injury and suffering**
- **Increase resources available to prevent, prepare for, respond to and recover from crises**
- **Increase ability and willingness to contribute to comprehensive defence**

Intentionally Blank

Chapter 3 —Comprehensive Defence Structure

This chapter presents principles and considerations for adjusting structures to enable greater private and civic sector participation in comprehensive defence.

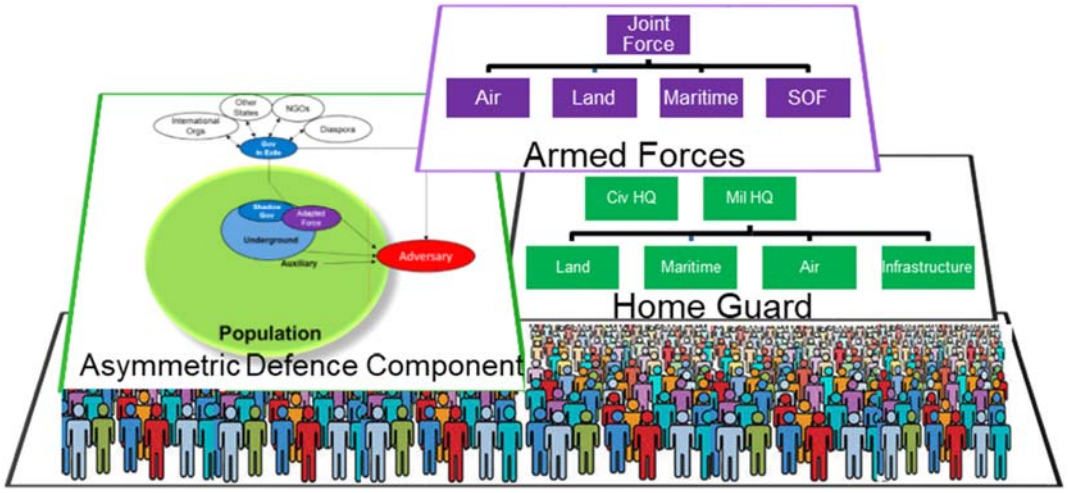


Figure 3.1 Integrated Layered Defence

Section 1—Overview

3.1 Comprehensive defence requires all sectors of society to be capable of integrating into a single, coherent, multi-layered system. However, governments are generally not designed to accommodate large-scale public participation in matters of national safety and security. Likewise, societies are not typically arranged in a manner that allows the public to easily contribute to national-level defence or emergency response efforts.

3.2 The discussion within this chapter offers three areas for consideration when organising to enable "the 98%" to contribute to a nation's defence. Recommendations for specific organisational structures are presented in the next two chapters.

- Organising Principles
- Deterrence and Response Layers
- Structural Categories

Section 2—Principles

3.2 The following principles should be considered when designing or adjusting comprehensive defence structures

- Whole-of Society Inclusion
  - ✓ To the greatest extent possible, organisational structures allow private and civic sector support and/or integration (Ch. 4, 5 & 14)

- Oversight
  - ✓ All comprehensive defence organisations and activities are pre-planned and officially sanctioned, in accordance with the nation's laws and policies (Ch 11)
- Multi-layered
  - ✓ All components of comprehensive defence are integrated to form a coherent, multi-layered deterrence and response system
- Multi-functional
  - ✓ Each comprehensive defence element is designed to protect against all widest range of threats possible
    - Multi-functionality must be supported by laws and policies (i.e., civil-military relations, military support to civil authorities, public-private partnerships, etc.)

Section 3—Layered Deterrence and Response

Table 3.1 Key Point: Multi-layered

Comprehensive defence provides a multi-layered deterrence and response system
1. Resilience **2. Standing armed forces and emergency response services** **3. Home guard** **4. Asymmetric Defence Component**

3.1 **First layer.** Resilience is the first line of defence

- The objective of the first line of defence is to prevent emergencies from occurring
- If an emergency does occur, the first line of defence allows the nation to quickly respond, while maintaining all critical services and functions
- Achieved through civil preparedness, military readiness, and whole-of-society integration
  - ✓ Civil preparedness decreases vulnerabilities (Ch. 17)
    - Reduce the chance of catastrophic accidents
    - Increases the ability to maintain critical services and functions in the event of an emergency
  - ✓ A well-designed whole-of-society, comprehensive defence deters aggression (Ch. 7)

3.2 **Second Layer.** Traditional response and regional defence organisations provide the second layer of defence

- Active and Reserve Components of Armed Forces
- Police
- Border Guard Services
- Emergency Response Organisations
- Intelligence Services
- Cyber Defence Organisations

3.3 **Third Layer.** The home guard, supported by private and civic society form the third layer
- Whole-of-society integrated support
- Home guard

3.4 **Fourth Layer.** The fourth layer is provided by the asymmetric defence component of the home guard
- Applies to defence against malicious acts, armed incursion in particular

Section 4—Structural framework

Table 3.-1 Structure Categories

Trained volunteers are the cornerstone of comprehensive defence
- **Full-Time Professionals**
- **Trained Volunteers**
- **Partially Trained Non-volunteers**
- **Untrained Non-Volunteers**

3.5 **Categories.** Comprehensive defence structures are divided into two major categories

- Full-time professionals
  - ✓ Includes components of Layer 2 (Par 3.2 above)
  - ✓ Formally committed to perform comprehensive defence functions
  - ✓ Includes private sector elements that are bound by law or contractual agreements
    - Contracted supplies and services
    - Critical infrastructure
- Trained volunteers[4]
  - ✓ Goal is for as many members of society as possible to be trained volunteers
  - ✓ Formally committed to perform comprehensive defence role
  - ✓ Not professional in the same sense as the standing services, but are trained, equipped and prepared to respond
  - ✓ Home guard members (Ch. 4)
  - ✓ Some members of Asymmetric Defence Component (Ch. 5)
- Partially trained non-volunteers
  - ✓ Capable of providing official support on short notice
  - ✓ Required training and education is provided through individual resilience measures (Ch. 2)
- Untrained non-volunteers
  - ✓ Goal of individual resilience and education initiatives is to minimize the number of untrained non-volunteers (Ch. 2)
  - ✓ More likely to require critical resources during a crisis

[4] Sometimes part of national obligation

✓ More likely to react spontaneously
- Will distract from coordinated whole-of-society efforts
- More prone to engage in vigilantism or criminal activities

Table 3.2 Key Take Aways--Comprehensive Defence Structure

➢ **Enable greater private and civic participation in comprehensive defence**
➢ **Increase resilience and deterrence by creating depth**
➢ **Reduce chances of counterproductive spontaneous reactions**

Chapter 4 –Home Guard

This chapter provides considerations for staffing, organising and equipping a home guard.

Section 1—Overview

4.1 A home guard can vary in capability from a part-time professional force to a group of trained, on-call citizens. The term is being used here to describe a government-led, voluntary or conscript organisation comprising members of the population who contribute to various aspects of their nation's safety and security. Per this definition, the home guard is the cornerstone of the nation's comprehensive defence volunteer structure, as it provides a reliable, practical means for organising, training and enabling private and civic sector participation in comprehensive defence.

4.2 The discussion within this chapter offers three areas for consideration when organising a home guard. Recommendations regarding training the home guard are contained in Chapter 6.

- Priorities and Responsibilities
- Key Considerations
- Equipping

Section 2—Priorities and Responsibilities

4.3 **Priorities.** In general, home guard responsibilities are prioritised as follows:

- Protect population
- Ensure continuation of essential goods and services
- Support emergency response and/or military operations

4.4 **Responsibilities.** Nearly all existing home guards are responsible for providing support to civil authorities as well as to the military. In keeping with that model, the following considerations apply.

- To the greatest extent possible, home guard units and members should be multifunctional
  - ✓ Capable of contributing to steady state resilience and also responding to natural, accidental and malicious events
  - ✓ Similarly, individuals may perform a particular function in peacetime and be assigned to a different home guard organisation during war
    - Example: a home guard unit may be designated to assist with mountain rescue in response to natural disasters and provide support to the military in the event of an armed incursion
- Detailed planning and coordination is required to ensure personnel and organisations are not mistakenly tasked to perform multiple functions at the same time

4.5 **Examples of home guard support to civil authorities**

- Police
  - ✓ Guarding and securing infrastructure
  - ✓ Movement control
  - ✓ Liaison functions
- Emergency Response/Rescue Services
  - ✓ Search and Rescue
  - ✓ Special expertise (medical, scientific support, etc.)
  - ✓ Manpower in support of disaster relief

The remainder of this section focuses on the home guard's responsibility to support the military, though many of the considerations are also applicable to other areas of comprehensive defence

Section 3—Key Considerations and Recommendations

4.6 **General**

- Establish active and reserve home guard structure
  - ✓ Active home guard maintains higher level of training and faster response times (See Chapter 6—Training)
- Even when organised by region, it is best to also align home guard units to specific military (and/or civil response) services
  - ✓ Home guard element in support of army, air force, navy, etc.
- Most effective if home guard elements are aligned with specific standing unit they support
  - ✓ Reinforces cohesion, continuity of effort, etc.
  - ✓ Helps prevent elements from being mistakenly multi-tasked
  - ✓ Elements can be realigned as necessary during any comprehensive defence phase
  - ✓ Notional example: Home Guard Company A supports the Army's 100th Airborne Brigade
- Home guard personnel can also individually augment civilian or military defence and security organisations (see Section 4.9)
- Include consideration for establishing mechanisms to support and encourage less obvious individual contributions
  - ✓ Emotional health call centres
  - ✓ Individual, non-professional assistance at healthcare facilities
  - ✓ Amateur radio hobbyists

4.7 **Legal** (see Chapter 11)

- Formally define relationships within law and policy
  - ✓ Delineate responsibilities
    - Particularly important if home guard lies outside of civil and military defence structures during non-crisis
  - ✓ Define intragovernmental relationships

- Home guard-MOI-MOD, etc.

✓ Establish procedure for legislative branch to appropriate and allocate public funds to the home guard
- Assign government entity to manage home guard funds (MOD, MOI, etc)

✓ Ensure ability for home guard to interface with Allies and international partners
- Nations often have domestic laws that prohibit their militaries from collaborating directly with members of a foreign population that have no official affiliation with their government, particularly on matters of defence and security
- Ensure home guard members are afforded adequate protections in the event of an armed incursion

4.8 Command and control (C2) (see figure 4.1)

 Include home guard representation at all levels of military force structure

✓ Representation may range from small liaison or advisory element to full headquarters

 Integrate standing armed forces personnel (active and/or reserve) into the home guard structure

✓ Common example: home guard commander and supporting element may be from standing active/reserve
- Provide senior leadership and C2 during crisis or conflict
- Responsible for overseeing home guard training and qualifications

✓ May also include a small, full-time, paid home guard element responsible for maintaining continuity and conducting various administrative and planning functions

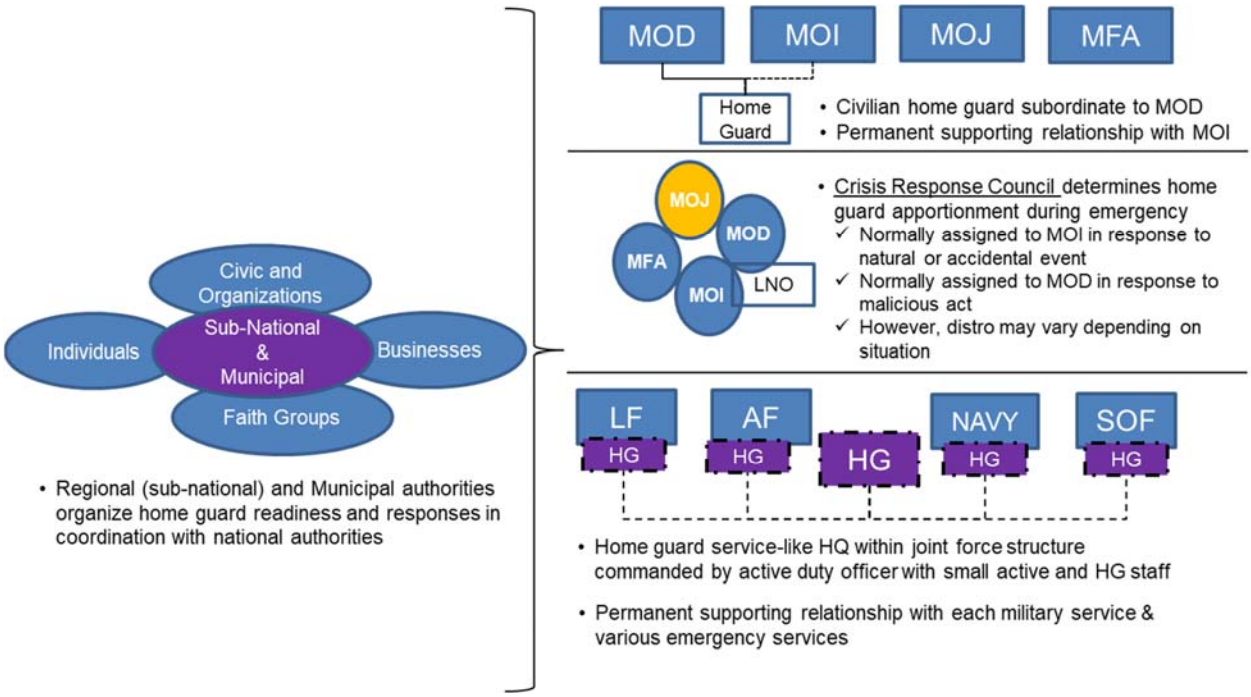


Figure 4.1 Home Guard Relationships

4.9 **Staffing Policies.** Consider voluntary contributions across all pillars, phases and threat categories (natural, accidental, malicious)

Table 4.1 Key Point: Staffing Considerations

- **Terms of service**
- **Qualifications**
- **Age requirements**
- **Social foundation**

- Common terms of service options
  - ✓ Active military service followed by long term home guard commitment (often to +/- age 50)
  - ✓ Short active conscripted military service for training (6-12 months) followed by long term home guard commitment (often to +/- age 50)
  - ✓ Completely voluntary
    - No prior service and no term commitment
  - ✓ Some nations use a blend of the three options by maintaining a primary and reserve home guard structure

- Incentives
  - ✓ Consider compensating unpaid volunteers for their expenses
    - Food while training
    - Travel costs

- Qualifications.
  - ✓ As a general rule, home guard service should be open to as many members of society as possible
    - Larger home guard creates greater deterrence
    - Larger network will be more secure when responding to malicious acts—more difficult to identify key members
  - ✓ Base selection and assignments on abilities vice disabilities
    - Do not disqualify persons solely for physical or mental conditions; i.e., “disabilities”
    - For the sake of social and psychological resilience, consciously seek volunteer opportunities for persons with disabilities
  - ✓ Allow public officials to serve (police, fire, armed forces, etc.)
    - Some will only be able to perform functions during peacetime, as their services may be required elsewhere during a crisis
  - ✓ Issues concerning discipline and/or security should be primary disqualifying factors
    - Past criminal behaviour
    - Potential to compromise security or collaborate with adversaries

- Age requirements
  - ✓ Normally 18 for support to military
  - ✓ Sometimes as low as 16 for non-military functions: i.e., natural and accident response

- Social foundation
  - ✓ Advocate and/or sponsor voluntary youth programmes that help prepare future home guard members and reinforce a sense of civic responsibility

Table 4.2 Key Point—Military/SOF Role in Home Guard Staffing

➢ Use military to help with screening and recruiting home guard personnel ➢ Involve SOF in screening and recruiting personnel for specialized tasks

4.10 **Assimilating volunteer organisations**

- Account for pre-existing groups that may be willing to perform comprehensive defence functions as well as groups that may be performing related functions that could be coordinated for better effect
- Establish procedures for integrating voluntary rescue and emergency preparedness organisations into home guard structures during crises
  - ✓ Organisations range from small local rescue groups to larger national organisations with headquarters and permanent staffs
  - ✓ May establish a national umbrella organisation to serve as a clearing house for all who wish to join or participate

Table 4.3 Best practice—integrating preparedness organisations[5]

Example of membership within one nation's umbrella voluntary professional rescue forum:
- People's First Aid and Rescue - Red Cross Emergency Service - Rescue Dogs - Caving Association - Scouting Emergency Group - Aero Club Flying Service - Amateur Radio Club • In this particular example, one permanent member represents the group in each police district • The nation also has several volunteer organisations that are not members of the forum

4.11 **Equipping.** Home guard units and members should be equipped according to their assigned (or anticipated) functions.

- Cost is the most significant consideration when establishing and sustaining home guards
- While surplus or non-standard equipment may reduce expense, it is also important to ensure the home guard is fully capable of performing its functions and is completely interoperable with the entity(ies) it supports

[5] Norway

- For nations within the NATO Alliance, defence-oriented home guard expenses count toward their defence investment requirement (i.e., 2% of GDP pledge)

Table 4.4 Home Guard Equipping Considerations

Types of equipment commonly issued to home guard elements **Individual equipment based on function** **Common unit equipment** ✓ Vessels ✓ Vehicles ✓ Rescue-related equipment ✓ Crowd control/marshalling (i.e., barricading; guarding) ✓ Communications ✓ Observation/surveillance
Storage considerations **Security** **Potential for misuse** **Facilities** **Maintenance requirements**
Storage options **Individually stored** **Unit stored** **Pre-positioned or cached** **Government stored**

Table 4.5 Key Take Aways--Home Guard

➢ Enables individuals and groups to contribute to comprehensive defence ➢ Increases depth by adding well-organised layer to nation's resilience, response and recovery capabilities ➢ Existence of a home guard deters aggression

Chapter 5 –Asymmetric Defence Component

This chapter provides considerations for forming and maintaining the nation's Asymmetric Defence Component.

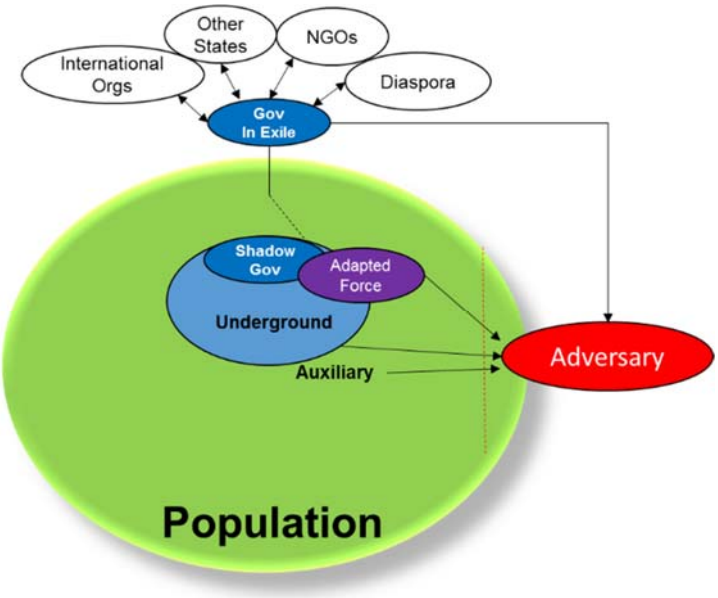


Figure 5.1 Asymmetric Defence Component Structure

Section 1—Overview

5.1 The Asymmetric Defence Component is an important element to the nation's first and fourth layers. In the event of an armed incursion, the ADC will provide the nation with the ability to conduct a government-led, whole-of-society resistance to re-establish independence and autonomy within its sovereign territory. This sense of the nation being "*indigestible"* serves as a strong deterrent to even the most powerful potential adversary.

5.2 The discussion within this chapter offers four areas for consideration when organising the ADC. Recommendations regarding training the ADC are contained in Chapter 6.

- Principles and considerations
- Structure and Functions
- Force Integration
- Responsibilities and Tasks

Section 2--Considerations

5.3 The principles and considerations that apply to comprehensive defence structures in general also apply to the ADC (see Ch. 2, Sec. 3). However, a few points warrant highlighting in specific context of building an ADC. A few others are unique to the ADC.

- Security (see Table 5.1)
  - ✓ Identities of ADC members must be carefully protected in all phases
    - Exposed members will almost certainly be put at risk by potential adversaries, even during peacetime
  - ✓ All members must be carefully screened
  - ✓ Security procedures must be formal and transparently codified in law and policy
    - Similar to approaches used to protect intelligence and law enforcement personnel
- Messaging
  - ✓ The fact that the ADC exists should not be kept secret
  - ✓ Publicly advertise that the nation has an ADC
  - ✓ Objective is to deter potential adversaries, reassure allies and partners, and reinforce social resilience among members of society
- Oversight
  - ✓ The ADC is an official, government-led organisation
  - ✓ An agency within the government should be assigned to lead planning, direction and oversight (see Ch. 14, Sec 2)
    - Often MOD or MOI-intelligence services
    - SOF will also play a large role
  - ✓ Loss or failure of government oversight during preparation or response phase risks the following
    - ADC networks and capabilities are used for criminal purposes
    - ADC networks and capabilities are used for nefarious political purposes
    - ADC efforts become uncoordinated, random and ineffective
- Whole of Society Inclusion
  - ✓ Most ADC members are volunteers from across society (the 98%)
    - This includes many ADC leaders
  - ✓ Government and ADC leaders must ensure all members abide by legal and ethical standards at all times

Table 5.1 ADC Lesson Learned—Security[6]

Security and messaging for deterrent effect must be balanced
• Compartmentalisation o Divide organisations into functional units (cells) o Limit information to cells to only that which is necessary for the mission o Cells should not know the identities or locations of members from other cells unless absolutely necessary

[6] ROC, pg 62-63

- Screening new members
  - Background checks are extremely important
  - Probationary period may also be appropriate
- Communications security
  - Train to communicate securely.
  - Assume all electronic communications to be monitored by the adversary at all times—peacetime/crisis/war
  - Calculate risk--there are numerous technical and non-technical means of communication, each with varying degrees of security, but few are 100% secure.
- Record keeping
  - Only record that which cannot be memorised and is required for future reference

Section 3—Section Structure and Functions

Table 5.2 ADC Lesson learned

If the ADC does not exist it cannot deter
The ADC should be organised, trained and equipped before a crisis begins

5.4 **Preparation Phase.** All elements of the ADC should be formed and maintained during peacetime (preparation phase), though they will not be fully manned.

- Maintain a small, centrally-controlled ADC core
- The size of the core should be based on a balance between security and responsiveness
  - ✓ The smaller the standing ADC, the longer it takes to screen, assess and assimilate enough volunteers to conduct effective defensive operations post-crisis
  - ✓ The larger the standing ADC, the greater the chance for security
- The ADC core's principal function is to increase and sustain resilience
- Leadership responsibilities should be executed by a cell within a lead agency, normally the MOD or the intelligence services of the MOI
- Other key personnel should be distributed across all sectors of society in accordance with their peacetime and/or crisis functions
- Tasks include defence planning, training and maintaining network infrastructure (recruiting, personnel management, etc.)
- Priority is on ensuring the ADC can rapidly assimilate volunteers in the event of a crisis

Table 5.1 ADC Elements

Underground (leadership)
Adapted Force (Combat)
Auxiliary (Support)
Public Component (Politics)

5.5 **Response Phase Organisation and Functions**. This section provides considerations for the ADC's structure based on response phase functions

- **Leadership and Command and Control** functions are performed by a cellular entity that remains within the home (occupied) nation
  - ✓ For the purpose of this handbook, the larger entity will be referred to as the **Underground** and the core leadership cell will be referred to as the **Shadow Government**
  - ✓ Civilian-led
  - ✓ A cell within the leadership element performs the functions of the head of government
    - This cell receives its guidance from the government in exile if one was formed
  - ✓ Secrecy and security are paramount, as this organisation is the nerve centre of the nation's defence apparatus
  - ✓ Draw from natural and experienced leaders
    - Former military personnel
    - Religious leaders
    - Teachers and professors
    - Local office holders
    - Neighbourhood representatives
    - University student leaders

- **Combat Actions** are conducted by a blended force, the exact composition of which varies by nation
  - ✓ Referred to in this handbook as the **Adapted Force**[7]
  - ✓ Determine composition based on overall national defence structures
    - May comprise elements of the nation's standing armed forces, reserve, home guard units, and volunteers from throughout the community (see Sec. 4 below)
  - ✓ Smallest of the ADC elements

- **Logistical and Operational Support** is provided clandestinely to the Underground and Adapted Force by a cellular organisation that is dispersed throughout the population.

[7] Often referred to as the Guerrilla Force because of the tactics it employs and the *in extremis* nature in which it is formed. However, when created as a component of a Comprehensive Defence, the force organised, trained and equipped as a standing component of the defence and security apparatus. Therefore, throughout this handbook, it will be referred to as the Adapted Force to recognise its composition: a combination of the traditional armed forces and predesignated elements of society.

- ✓ An individual cell may consist of a group or a lone person
- ✓ A cell may be asked to carry out a single task (deliver a message, switch on a light), a continuous mission (provide medical treatment as required), or circumstances may be such that they are not called upon at all during the entire course of the conflict
- ✓ Part time volunteers who consciously accept the risk associated with the functions they agree to perform in the event of an armed incursion
- ✓ For added resilience, only provide members the information required to perform their task
  - Members should not be aware of the "big picture"
- ✓ Generally the ADC's largest element and strongest link to the population
- ✓ Referred to as the **Auxiliary**

- **Overt Political Expressions** within occupied territory(ies) are the responsibility of the **Public Component**.
  - ✓ If there is no exiled, displaced or shadow government, the Public Component may perform the national leadership function
  - ✓ Otherwise, it is an extension of the existing government
  - ✓ May take the form of opposition parties, trade unions, etc.
  - ✓ The Public Component's ability to function will vary based on the occupying power's level of tolerance for political opposition
  - ✓ If not allowed to express political opposition, the component should relocate and/or the ADC should conduct political opposition activities clandestinely through existing organisations

5.6 **Popular Participation**. Most of the population will not belong to either of the active elements of the defence structure described above

- They are, nevertheless, capable of contributing to comprehensive defence through low risk, passive activities
- Enable popular participation by educating, informing and including society in the planning process
- A properly trained underground will be able to organise and guide public participation
- The objective is to inhibit the occupying force's ability to consolidate power

Table 5.3 Key Point—ADC Relies on the Population

The ADC relies heavily upon the population The largest element of the ADC (the Auxiliary) is composed almost entirely of members of the population

Section 4—Force Integration

5.7 **Considerations.** Integrating the ADC into the larger defence structure is particularly challenging and deserves continuous attention during the preparation phase

- All components of the armed forces and the ADC must train together regularly
  - ✓ This is particularly important during the first several years after establishing the ADC
- Include the ADC in all international exercises so partners and allies become accustomed to operating alongside asymmetric forces
- Train and educate leaders at all levels in the nuances of employing the ADC
- Clearly specify the relationship between the ADC and other elements of the armed forces
- The construct decided upon will influence command and control structures, as well as training and equipping requirements
- The relationship is generally designed according to one of the following two models:
  - ✓ 1) ADC and standing armed forces are fused into a single entity
    - ADC is commanded by an element of the armed forces
    - Most often, the command element is from the nation's SOF
  - ✓ 2) ADC operates alongside the armed forces based on a "supporting – supported" relationship

Table 5.4 Force Integration Lesson Learned

Senior leaders often cite scheduling conflicts as a reason for not participating
Untrained leaders will be incapable of effectively fulfilling their required comprehensive defence responsibilities

Section 5—Responsibilities and Tasks

5.8 General Responsibilities and Tasks

- Specific ADC responsibilities and tasks will be based largely on the results of the assessment and capabilities development portions of the Comprehensive Defence Planning Process (Ch. 16).
- The following tables provide examples of common responsibilities and tasks

Table 5.5 ADC component potential responsibilities

Element	Responsibilities
Underground	• Intelligence and Counter Intelligence Networks • Subversive Radio Stations • Media networks (print shops, newspaper, social media, television, web pages) • Materiel control: identifications, explosives, weapons, munitions • Networks for moving and protecting personnel, generating funds • Conducting acts of sabotage in urban centres • Operating clandestine medical facilities

Element	Responsibilities
Auxiliary	• Logistics procurement and distribution • Labour for special material fabrication • Security and early warning for underground facilities • Intelligence collection • Recruitment • Communications network staff, such as couriers and messengers • Media distribution • Safe house management • Logistics and personnel transport
Adapted Force	• Conduct military operations as directed by the government via the underground

Table 5.6 ADC potential tasks

Functional Area	Potential Tasks
Sustainment	• **Storage and distribution of supplies** • **Medical treatment services** • **Equipment maintenance** • **Secure materials rationed or prohibited by occupying power (secret confiscation)** • **Battlefield recovery of weapons, ammunition, etc. (adversary and friendly)** • **Construction** o Fortifications o Safe havens o Routes and crossings
Movement and Manoeuvre	• **Direct and indirect combat operations** o Employing unconventional (irregular) tactics • **Transportation** o Non-standard (civilian) air, land and maritime possibilities o Pack animal • **Route reconnaissance** • **Emplacing or removing obstacles** o Routes, landing zones, etc.
Intelligence	• **Enemy force composition, disposition, strength and intentions** • **Terrain analysis** o Trafficability o Ability to support logistical sites, etc. • **Political information** • **Data related to potential targets**
Fires	• **Spotting and observing fires** o Performing joint fires observer (JFO) functions • **Battle damage assessments (friend and foe)**
Protection	• **Providing quarter and safe houses** • **Equipment cache** • **Identity documents**

Functional Area	Potential Tasks
Information and Communications	• Reinforce strategic communications message • Provide ISPs technical platforms • Provide courier support (i.e., message delivery)

Table 5.7 Key Take Aways—Asymmetric Defence Force

- **Provides strong deterrent against malicious acts**
- **Must be deliberately planned in advance**
- **Formal government oversight critical**
- **Security is paramount**

Chapter 6 —Comprehensive Defence Training

This chapter provides considerations for designing and conducting comprehensive defence training.

Section 1—Overview

6.1 To facilitate resilience and deterrence, comprehensive defence training must be designed to regularly test and improve capabilities across all six pillars. Additionally, a single training activity may serve multiple strategic purposes: reinforce national pride, reassure partners and allies and deter potential aggressors. All three purposes should be considered and prioritised when planning and executing training activities.

6.2 The discussion within this chapter focuses primarily on training designed to deter and respond to malicious acts. Considerations for the following five topic areas are offered.

- Principles and considerations
- Private and Civic Sector –volunteers
- Home guard
- Drills and Exercises
- Asymmetric Defence Force

Section 2—Considerations

6.3 The following considerations apply to several or all sectors of society

- Ensure training is closely linked to individual resilience education (Chapter 2)
- Design and execute all training with a high level of professionalism and intensity
  - ✓ Develop a systems approach to training for the home guard and ADC
  - ✓ Develop qualification requirements and standards
- Determine frequency based on readiness requirements, deterrence objectives and population size (i.e., annually, every three years, etc.)
- Seek to involve every member of society
  - ✓ Encourage members of the population to provide training venues (ranges, training areas, classrooms, etc.)
  - ✓ Rotate training activities among regions to facilitate local participation
  - ✓ Include private and civic sector representatives when designing training
- With the exception of conscription, members of the private and civic sectors cannot be compelled to participate in defence training beyond that which is included in the nation's public education curricula or laws governing businesses
  - ✓ Consider budgeting for and compensating those who participate in defence training as well as developing non-monetary incentives
    - Develop laws that support time off work for training, etc.
- Use all possible methods of delivery (Table 6.1)

Table 6.1 Considerations for Training Methods

Method	Considerations
School Curriculum	☐ Reinforce resilience by incorporating comprehensive defence into civic studies ✓ Topics relevant to social and psychological resilience (Chapter 5) ✓ National Concept for Comprehensive Defence ✓ Legal and ethical behaviour in the event of an armed incursion ✓ Security considerations—balancing secrecy with transparency ✓ Communications methods if invaded
Online Courses	☐ Non-sensitive subjects only ☐ Easily accessible ☐ Self-paced ☐ Relatively low manpower requirement ☐ Useful for general knowledge and prerequisite courses ☐ Limits cell member exposure ☐ Unless specific security measures are implemented, assume adversaries have access to training material and can determine specifically who is receiving the training
Decentralised	☐ Use “train the trainer” approach to develop distributed pool of instructors ☐ Approved instructors deliver at regional or local venues ☐ May be supported by community groups and associations ☐ Limits ADC cell member exposure
Consolidated	☐ All training conducted at one or limited number of venues ☐ Ensures continuity and interoperability ☐ Less secure—all participants known ✓ Not well-suited for ADC
Exercises	☐ Promotes interoperability ☐ May use to reinforce individual skills, collective skills or both ☐ Must consider risk of exposing ADC members ☐ Individual training can be incorporated into exercises ☐ Determine frequency based on training requirements ☐ Use as an opportunity to enhance Military Assistance skills ☐ Consider table-top and computer-generated simulations for senior officials

Section 3—Private and Civic Sector

6.4 Private sector

☐ Identify key functions and preeminent organisations responsible for the functions
- ✓ Telecommunications
- ✓ Transportation
- ✓ Printing services
- ✓ Food and water
- ✓ Port authorities
- ✓ Construction
- ✓ Banking

☐ Identify and clarify expectations for public-private relationships and interaction at all levels

- Account for private sector training with law enforcement agencies, border guard, emergency services, etc. at each of those levels
  - ✓ Local
  - ✓ Sub-national
  - ✓ National
- Identify and reinforce areas of shared private-public interest
  - ✓ Example: Design professional continuing education to benefit the business and comprehensive defence efforts
    - Link safety and security training to counter terrorism, cyber defence, etc.
  - ✓ Coordinate with businesses when designing home guard training
- Encourage private sector to incentivize their employees to participate in comprehensive defence training
  - ✓ Work release
  - ✓ Special recognition

6.5 Civic Sector

- Identify civic sector training interests
  - ✓ Design training to reinforce marketable skills and hobbies
    - Cyber
    - Construction methods
    - Medical
    - Civilian clubs (see Table 4.3)
- Volunteers will train as part of home guard or ADC
- Encourage non-volunteers to participate in drills and exercises
  - ✓ Role players
  - ✓ Allow land to be used
  - ✓ Expert advisors

Table 6.2 Key Point--Detailed Training Requirements

Detailed home guard and ADC training requirements will depend on force structure, assigned functions and planned methods of employment, all of which will be based on how the nation anticipates an armed incursion may unfold.

Section 4—Home Guard

6.6 The following five questions are used to frame considerations related to training that is specific to the home guard

- Who Trains the home guard?
  - ✓ As often as possible training should be conducted by and with the aligned entity (emergency response, civil preparedness, military, etc.)
  - ✓ Allow home guard members to attend the formal schools used by their aligned element

- ✓ Assign active duty or reserve personnel to home guard units as commanders, trainers and/or advisors

- Where does the home guard train?
  - ✓ Government facilities (local, sub-national and national)
  - ✓ Private property made available by citizens
    - Outdoor areas (farms, etc.) or indoors (conference rooms, auditoriums)
    - Also contributes to deterrence by demonstrating private and civic sector support and resolve
    - Often overlooked as potential volunteer function

- What common skills do all home guard members require (see Vol II, Ch 5)
  - ✓ Reporting
    - Identify adversary equipment, uniforms and activity
    - Distinguish and report critical information
  - ✓ First Aid
    - Render first aid to self
    - Render first aid to others
  - ✓ Storage
    - Hide material; i.e., constructing and managing cache sites
  - ✓ Survival
    - Store and find food
    - Store and find water
    - Map reading & land navigation
    - How to conduct self in occupied territory
  - ✓ Communications
    - Communications security
  - ✓ Cyber security

- How much training do home guard members receive
  - ✓ Conscripted home guard members receive basic skills training during their 6 – 12 month tour of conscripted service
  - ✓ Example for non-conscripted active home guard
    - 100 hours basic training in first year (normally a single two-week period)
    - Additional 200 hours training required during the following two years
    - 48 hours per year to maintain active service
    - Additional hours for annual weapons training for those who are issued weapons
    - Case studies show members commonly opt to exceed minimum training requirements

Section 5—Drills and exercises

Table 6.3 Home guard lesson learned

Seek to involve as much of the population as possible in home guard drills and exercises

6.7 Because of their visibility, drills and exercises are particularly useful for serving all three comprehensive defence strategic purposes

- Reinforce national pride
- Reassure partners and allies of nation's resolve
- Deter potential aggressors

Table 6.4 Key Point--Home Guard Training

A well-trained part-time volunteer force can quickly integrate and support its aligned government entity

6.8 **Drills**

- The term drill is being used here to refer to short duration events designed to test specific capabilities
- The most common drill would be a no-notice recall
- For nations with home guards, drills to test communications and emergency response notification systems are extremely important
- When testing systems and procedures associated with malicious acts, communications security becomes particularly important

6.9 **Exercises**

- Exercises last longer than drills and designed to improve current capabilities or develop new capabilities
- Local or regional exercises
  - ✓ 2-3 day duration is normally sufficient
  - ✓ Encourage non-volunteers to observe, and where possible, participate
    - Increases the ability of non-volunteers to contribute
    - Serves as a recruiting tool
- National and international exercises
  - ✓ A common mistake is to fail to account for home guard in large-scale exercises
  - ✓ Be prepared to modify software and other exercise design tools
  - ✓ Include home guard to ensure all components of the defence understand how to interact
    - Failure to include home guard in exercises will lead to confusion in a real-world situation
  - ✓ Ensure international partners and allies also understand the implications of operating among home guard forces

6.10 Whether designed to support responses to malicious or non-malicious acts, drills and exercises are normally conducted to test and improve some combination of the following capabilities

6.11

Table 6.5 Common home guard drill and exercise objectives

Capability	Audience
Alert	• Public • Government • Home guard
Assemble	• Government • Home guard
Coordination and decision making responsibilities	• Government • Home guard
Coordinate communications with civilian population	• Government • Home Guard
ID adversarial information operations/responses	• Government • Home Guard • Public

Table 6.6 Sample Design for 3-Day Home Guard Exercise

Context	☐ Nation conducts a biennial regional exercise with each of its six regions
Concept	☐ From 1 – 3 June 2034, conduct regional exercise in order to re-familiarise the population of Region 3B with the nation's approach to Comprehensive Defence, refresh home guard individual and collective skills and enhance integrated force C2 capabilities
Day 1. Individual skills training using rotating station method	☐ **Integrity, ethics and law** ✓ Include in all training ☐ **Move** ✓ When attached to the armed forces (helicopter, watercraft, foot, vehicle, etc.) ✓ When operating separately from armed forces ☐ **Shoot** ✓ Include training on potential adversary weapons ☐ **Communicate** ✓ Security is paramount ☐ **Medicate** ✓ Tactical Combat Casualty Care ☐ **Selective specialty functions**
Day 2. Collective training using rotating station method	☐ **Collective tasks** ✓ Team or cell functions ☐ **Interoperability with aligned element(s)** ✓ Accomplishing tasks with two or more units/cells
Day 3. Live exercise, culminating with community social event and static display	☐ **Respond to alert and notification process** ✓ Security/avoiding compromise ✓ Improving response times ☐ **Link-up procedures** ✓ Linking up with fellow home guard members ✓ Linking up with armed forces ✓ Linking up with private sector (e.g., critical capability providers) ☐ **Exercise command and control**

Section 6—ADC training considerations.

6.12 The following considerations are particularly important when designing and conducting training for the ADC. Several of the points will apply to other training audiences as well.

- ADC must exercise capabilities regularly
- Only key personnel within the core element need to participate in exercises
  - ✓ Develop methods for cell leaders to communicate with and train their cell members
- Be careful not to expose ADC membership
  - ✓ Training events and activities do not need to be visible
  - ✓ Use broad, redundant alert and recall procedures
    - Seemingly generic public radio and TV messages
    - Mass text messages to entire population
  - ✓ Do not direct movement to location or by method that will make identify/function obvious

Table 6.7 Key Point--Integrating ADC into Training

It is imperative that the ADC be considered in all conventional training, to include table top exercises and simulation Modification to exercise scenarios and simulation software will be required

6.13 **General training considerations by entity**

- Military
  - ✓ Integrate “Resistance” scenarios into all exercises
    - Modify simulation capabilities as required; i.e., gaming software, etc.
  - ✓ Adapt training and education curricula to account for comprehensive defence (Chapter 2)
    - Decentralised and distributed command and control of cellular structures
    - Interacting with uncommitted element of the civilian population
  - ✓ Train conventional forces to integrate with, support and/or operate alongside ADC

6.14 **Civilian Ministries**

- Rehearse transitioning from Preparation Phase to Response Phase
  - ✓ Identify functions and organisational structures that change when transitioning
    - Cells that exist within other organisations, etc.
- Security measures
- Operating within the Underground structures
- Performing functions directed by the occupying power
  - ✓ Elements of the government that are left in place will need to cooperate with the occupying forces, either to ensure essential services continue or to deceive the occupying power
  - ✓ Plans and provisions for this should be rehearsed in advance

6.15 Civic Sector

- Basic individual and unit (cell) skills training for unassigned volunteers
  - ✓ Establish common baseline capability
  - ✓ Use standing armed forces to deliver basic skills training
    - SOF and conventional forces
- Advanced and specialty skills associated with specific functions
  - ✓ Use SOF to deliver advanced and specialty training
- Encourage members of the population to serve as role players during training
  - ✓ Do not need to know the "big picture"
  - ✓ Do not need to make a formal, long term commitment
- Auxiliary functions (medical, storage, document production, etc.)

6.16 Private Sector

- Voluntary financial support
- Materiel support (example: boats for volunteer coastal watchers, armbands for Adapted Force when conducting operations, etc.)
- Facilities (ranges, training areas, classrooms, etc.)
- Auxiliary functions (medical, storage, document production, etc.)

Table 6.8 Key Take Aways--Training

- **Seek to involve all members of society**
- **Ensure training is consistent and demanding**
- **Balance security with deterrence messaging**

Chapter 7 Deterrence

This relatively short but important chapter presents considerations for enabling society's role in deterrence through comprehensive defence.

Section 1—Overview

7.1 The primary purpose of comprehensive defence, from the perspective of malicious acts, is to generate peace through deterrence. However, to be effective, society must be consciously involved in demonstrating and communicating the nation's defensive capabilities.

Government initiatives to educate, inform and enable the population to defend against malicious attacks increase resilience and deter aggression

- **An adversary is less likely to expend resources on a malicious attack if the public is capable of detecting or neutralizing the action and its effects**

Section 2—Framing Deterrence.

7.2 Two types of deterrence
- Denial—prevents enemy from achieving objective
- Punishment—costs to the enemy will outweigh any benefits
  - ✓ Normally implies counter-offensive action, but not necessarily
  - ✓ Comprehensive defence can be used to impose heavy costs upon the adversary

7.3 Three components to deterrence
- Credibility—willingness to take action
- Capability—the ability to impose cost on the adversary
- Communication—two-way understanding and perception that informs cost-benefit calculations on both sides

Section 3—Considerations for Enabling Society's Participation

7.4 Desired State. Society is willing and capable of contributing to comprehensive defence's deterrent effects.
- Credibility
  - ✓ Conduct well-organised exercises and drills
  - ✓ Facilitate public threat awareness
  - ✓ Publicise public commitment to and understanding of comprehensive defence
- Capability
  - ✓ Make smart investments
    - Home guard and ADC must be properly equipped
    - Incentivize participation in training
    - Conduct thorough Comprehensive Risk Assessments

- Communication
  - ✓ Deterrence communication involves watching *and* listening
  - ✓ Implement measures designed to "read" potential adversary(ies)
  - ✓ Understand potential adversary's intentions
  - ✓ Gauge the effects of own deterrence actions
- Develop simple approach to **strategic communications**
  - ✓ Themes: An overarching concept or intention designed for a broad application
    - Our population will defend itself if attacked
    - The aggressor will ultimately lose at great cost to themselves, because we have made ourselves indigestible
  - ✓ Messages: Narrowly focused communication directed at a specific audience
    - This exercise demonstrates our willingness and increases our capability to defend ourselves
  - ✓ Coordination
    - Ensure society knows and understands the themes and narrative
    - Ensure messages are coordinated among stakeholders
  - ✓ Actions must support themes and messages
    - Actions are the strongest form of communication
    - Balance security with strategic communication

Table 7.1 Key Takeaway--Deterrence

The primary source of comprehensive defence's deterrent power is not weapons or technology. It is society. Thus, to serve as an effective deterrent, society must be fully considered and specifically enabled to contribute to all aspects of comprehensive defence.

Chapter 8 Malicious Acts: Weaponised Information, Cyber Attacks, and Terrorism

This chapter offers considerations for defending against three types of malicious acts distributed across the spectrum of conflict: cyber attacks, weaponised information, terrorism and other irregular violent attacks.[8]

Section 1 – Malicious acts overview

8.1 The chapter presents measures the government can implement to enable the public to take actions that will prevent or mitigate the effects of the malicious acts described below. The references provided alongside the considerations lead to sections within the handbook that contain further details and checklists for preparing the population to perform the functions described here.

8.2 The information presented here is meant to be used in conjunction with the corresponding sections in Volume II.

8.3 **What are Malicious Acts?**

- Any action perpetrated by an external entity, the effects of which threaten the targeted country's safety, security, sovereignty or its peoples' right to self-determination.
- Malicious acts need not be violent or physical. Weaponised information or nefarious cyber activity may undermine a nation's independence more effectively over time than an armed invasion would. In short, malicious acts include unambiguous, overt acts of aggression, as well as hybrid breaches of the nation's sovereignty.

8.4 **Enabling the 98%.** The civic sector's potential to make significant contributions to defending against malicious acts is often overlooked. National constructs are customarily designed to protect civilians by totally isolating them from the effects of malicious acts. According to these common models, preparation and response fall solely within the purview of the state's defence and security services. Thus, for many nations, organising Comprehensive Defence against malicious acts requires special focus and attention.

8.5 **Non-Malicious Acts.** As noted in Chapter 1, the Comprehensive Defence Handbook focuses primarily on malicious acts. However, per the considerations

[8] This handbook uses the NATO definition for terrorism: "The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives." However, this definition is not universally accepted. So, the term terrorism, as used in the handbook, also refers to irregular armed attacks, meaning events in which the motive, target or method of attack may not meet an agreeable definition for terrorism, but have the same effect on the population.

below, many elements of the checklists that follow apply equally to malicious and non-malicious acts:

- Non-malicious acts include natural and accidental events
  - ✓ Natural disasters, pandemics, and other incidents that occur without a deliberate, malicious intent driving them
  - ✓ These events are often unpredictable and spontaneous in nature.
- Non-malicious acts require preparedness assessments and planning that incorporates civil society, the private sector and government
  - ✓ Approaches should be integrated with those developed and implemented to address malicious acts
  - ✓ Therefore this handbook and checklists within can be applied to either type of act.
- Many of the preventative measures, responses and results are the same for malicious and non-malicious acts.
- Non-malicious acts can be leveraged or exploited by state or non-state actors to further their interests
  - ✓ This must be considered and closely monitored in response and recovery phases
- A malicious act will often appear to be a non-malicious accident (gas plant explosion, massive power outage, etc.)

Section 2—Defence Against Weaponised Information

Table 8.1 Disinformation Key Lessons Learned

➢ **Education commencing in primary school is the most effective defence**
➢ **Education programmes should be focused on "how to think" "not what to think"**
➢ **Augment education with information campaigns that highlight the threat**

Figure 8.1 Sample resource for teaching the public to spot disinformation[9]

8.6 **Overview.** Due in large part to modern technology, societies are constantly threatened by disinformation. Nefarious attempts to influence elections and exploit social and ethnic fault lines have come to define our modern world. Whether projected by state actors, malign non-state organisations, or a mischievous juvenile with a laptop computer, weaponised information can have a destabilising effect on governments and societies alike.

8.7 Most states have an array of tools at their disposal to help them identify, attribute and respond to weaponised information. Many of these resources reside in the intelligence community and are not available to the public. However, some nations have successfully integrated public education and information campaigns into their comprehensive defence approaches. As a result of the steps taken in those countries, private and civic sector awareness of weaponised information has increased, as has the population's ability to recognise and help counter it.

8.8 Below are specific steps governments can take to educate, inform and enable the population to participate in a whole-of-society defence against weaponised information.

- Educate
  - ✓ Develop curricula to teach students to recognise disinformation (Vol I, Ch 2)
    - Details and approaches may vary by region and municipality, but objectives should be uniform
  - ✓ Critical thinking forms the foundation (Vol II Ch 3)

[9] https://www.ifla.org/publications/node/11174

- ✓ Begin in primary school and continue through all levels/grades[10]
- ✓ Provide advanced training for educators and curriculum developers[11]
- ✓ Establish online and public media-based training and information programmes for general society
- ✓ All programmes and information must be apolitical
  - Any perception of government manipulation will alienate the population
  - All messages and actions should reinforce the principle of governance by consent

- Inform
  - ✓ Make population aware of available resources
    - Fact-checking software and websites[12]
    - Online training sites

- Enable
  - ✓ Publish simple approach to spotting disinformation (Fig 8.1)
  - ✓ Involve community in programme development (Vol II, Ch 3)
    - Sponsor public and student contests
  - ✓ Establish cooperative agreements with governments and private corporations (Table 8.3)
  - ✓ Engage international subject matter experts
    - Corporations will act as filters, while respecting free speech
    - Tech companies, media outlets, etc.

Table 8.2 Key Point—Military role in enabling society to counter disinformation

Consideration should be given to including the military in public-private and civil-military partnerships and training programmes

- ➢ Military education contains a significant focus on "hybrid tactics," to include recognising and countering disinformation
- ➢ Particularly true for Special Operations Forces

[10] Site contains references for teachers https://teachingkidsnews.com/fakenews/
[11] The following links lead to useful considerations for developing curricula and training tools https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1346&context=jmle and http://eprints.lse.ac.uk/101083/6/Disinformation_digital_literacy_and_the_school_curriculum_updated_Sept_2019_.pdf and https://cor.stanford.edu
[12] It is important, also, to ensure that fact checking sites are unbiased

Table 8.3 Sample public-private cooperative agreement[13]

European Union Code of Practice Against Disinformation

- Disrupt advertising revenue for accounts and websites misrepresenting information and provide advertisers with adequate safety tools and information about websites purveying disinformation.
- Enable public disclosure of political advertising and make effort towards disclosing issue-based advertising.
- Have a clear and publicly available policy on identity and online bots and take measures to close fake accounts.
- Offer information and tools to help people make informed decisions, and facilitate access to diverse perspectives about topics of public interest, while giving prominence to reliable sources.
- Provide privacy-compliant access to data to researchers to track and better understand the spread and impact of disinformation.

Section 3—Enabling the 98% to Contribute to Cyber Resilience and Defence

Table 8.4 Cyber Key Lessons Learned

- **Develop education programmes to raise cyber awareness and increase the pool of cyber experts**
- **Implement programmes to keep society informed of looming cyber threats**
- **Establish public-private partnerships to protect critical data and cyber-dependent infrastructure**

8.9 **Overview**. The cyber domain is often the first line of contact with an adversary. In addition to attacking critical infrastructure, a potential enemy can easily access and seek to influence the general population through cyberspace without violating any physical protocols.

8.10 The main asset to focus on and to take into consideration in order to protect people from threats coming from and within the cyber domain are the people themselves. If an administration/organization continually reacts to every new type of attack, that administration/organization will always be one step behind and therefore inevitably get compromised.

[13] EU Code of Practice on Disinformation is an example. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

8.11 **Desired State**. Below are steps the government can take to educate, inform and enable the population to contribute to increased cyber resilience.

- Education (Ch 2)
  - ✓ Develop partnerships with industry and academia to promote cyber security education at all levels
  - ✓ Embed cyber security and digital skills in relevant courses within the education system, from primary to postgraduate level
- Information
  - ✓ Publish and promote cyber awareness handbook
  - ✓ Update the public routinely on cyber threats[14]
- Enable (Ch 5)
  - ✓ Integrate a cyber defence plan into the national comprehensive defence strategy[15]
    - Give clear guidance on who is responsible for what and why
    - Should include purposes, definitions, roles and responsibilities to strengthen the national cyber structure
  - ✓ Establish a central authority responsible for cyber governance
    - Responsible for guidance and coordination
    - Link between the political sphere and comprehensive defence environment
  - ✓ Establish response teams following the CERT/CIRT/CSIRT/SOC model[16]
  - ✓ Develop clearly defined partnerships with companies that manage Critical National Infrastructure (CNI)
  - ✓ Identify public and private entities that provide essential and/or digital services to society
    - Include, inter alia, entities that provide e-commerce, cloud computing or search engine services that are headquartered or have representative offices within the territory of the country
  - ✓ Encourage companies that do not operate essential digital services to voluntarily notify the national response team of incidents that may impact continuity of their services
    - The objective is to develop a culture of awareness and information sharing
  - ✓ Establish a single authoritative online point of advice on responding to cyber threats[17]

---

[14] https://staysafeonline.org/wp-content/uploads/2018/09/SMB-Toolkit-FINAL.pdf
https://arcticwolf.com/wp-content/uploads/Cybersecurity-Awareness-Handbook.pdf
[15] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
[16] Computer emergency response team (CERT) computer incident response team (CIRT), computer security incident response team (CSIRT), security operations centre (SOC):
https://resources.sei.cmu.edu/asset_files/WhitePaper/2007_019_001_294579.pdf
https://searchsecurity.techtarget.com/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference
[17] https://getsafeonline.org/

- ✓ Establish a cyber skills advisory group comprising government, employers, and academia to routinely assess and provide guidance on improving critical cyber security skills
- ✓ Develop opportunities for collaboration in training and education between government, the Armed Forces, industry and academia, together with facilities to maintain and exercise skills
- ✓ Develop better understanding of the cyber security industry's strengths, growth potential and barriers to success
- ✓ Encourage industry-led standards and guidance that are readily used and understood

Table 8.5 Military role in preparing society to defend against cyber attacks

- ➢ Nations invest heavily in military cyber defence infrastructure and training
- ➢ As with weaponised information, this too is particularly true for SOF
- ➢ Here too, consideration should be given to including the military in cyber-related public-private and civil-military partnerships and training programmes

Section 4—Comprehensive Defence against Terrorism

8.12 **Overview.** The physical impacts of terrorist attacks, natural disasters and accidents are often similar. The following section, therefore, concentrates on highlighting the two notable differences when preparing comprehensive defence against terrorism versus other threatening phenomenon: 1) the specific actions the government can take to enable members of society to detect and prevent and respond to terrorist acts, and 2) additional assessment considerations.

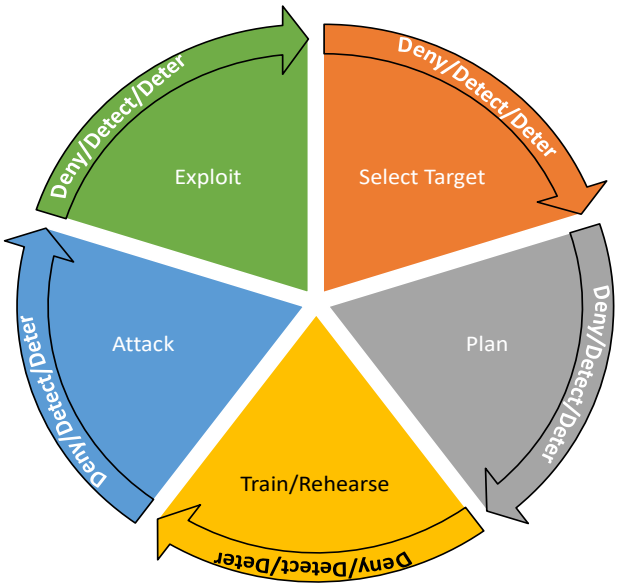


Figure 8.2 Terrorist attack cycle

8.13 **Society's role**. Private and civic sector contributions to comprehensive defence against terrorism are aimed toward denying terrorists access to information and potential targets, detecting their attempts to gain information and access, and ultimately deterring attacks should the terrorists gain information and access to the target. Should efforts to deny, detect and deter ultimately fail, members of the population must be capable of responding in a way that will contribute to a whole of society effort, or at least not make matters worse.

8.14 **Desired State.** Individual members of society able to contribute to national efforts to defend against terrorism and other irregular violent acts.

- To facilitate a whole-of-society defence against terrorism, the government should focus its effort on educating, informing and enabling the public to perform actions listed above (deny, detect, deter, respond). The steps taken to adapt the interagency coordination infrastructure and organise society will also contribute to this objective (see Ch. 14).
- Table 8-6 contains specific actions the government can take to implement a comprehensive approach to defending against terrorism. The following are lessons learned and best practices used to increase whole of society resilience against terrorist threats. (See Vol II for recommended public actions).

Table 8.6 Preparing society to defend against terrorism

Enabling capability or action
Educate (Vol II, Ch 3) • **Establish programmes to educate the public on the following:** o Phases of a terrorist attack o Terrorist actions during the Target Selection, Planning and Rehearsal phases ▪ For example—internet searches, physical reconnaissance, dry runs to test security and attack techniques o Identify radicalisation and signs of extremism • **Example 1: NATO Counter Terrorism Reference Curriculum**[18] o Provides sample CT curriculum, with references o Contains four themes, each of which is sub-divided into blocks and modules o Available online free of charge ▪ Theme 1: Introduction to Terrorism ▪ Theme 2: Understanding Ideologies, Motivations & Methods ▪ Theme 3: Contemporary Challenges & Evolving Threats ▪ Theme 4: Counter-Terrorism: Strategy, Operations & Capacity Building • **Example 2: Danish Civil Society Empowerment Programme**[19] o "…empowers (civil society, grass roots organisations and credible voices) to provide effective alternatives to the messages coming from violent extremists and terrorists, as well as ideas that counter extremist and terrorist propaganda" o Includes training material for developing online counter and alternative narrative programmes o Slide presentations with notes in 20 EU languages ▪ Creating online campaigns around counter and alternative narratives ▪ Campaigns ▪ Lessons learned ▪ Target audience • **Example 3: UK ACT Awareness E-Learning**[20] o Designed for use by private and civic sector (employee scenarios) o Six Modules ✓ Intro to Terrorism ✓ Identifying Security Vulnerabilities ✓ How to ID and Respond to Suspicious Behaviour ✓ How to ID and Deal with Suspicious Item ✓ How to Respond to Firearms or Weapons Attack ✓ Summary and Supporting Materials o Interactive o Free, easily accessible via internet o Generates a completion certificate

[18] https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200612-DEEP-CTRC.pdf
[19] https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network/civil-society-empowerment-programme_en
[20] https://ct.highfieldelearning.com/

Enabling capability or action

- **Example 4: US DHS "If you see something say something"** [21]
  - Public education and awareness programme: "PSA: Take the Challenge"[22]
  - Includes set of interactive videos that teach awareness

Inform

- **Make the public aware of likely terrorist targets**
  - Develop system to regularly inform private businesses that host large crowds, or manage critical infrastructure or critical functions
- **Use alert level warnings wisely** (i.e., red, orange, yellow, etc) [23]
  - Too many warnings sent too frequently can desensitise the public
  - Focus warnings in terms of time, location, possible outcome
  - Provide instructions along with warnings
- **Make sanction lists with names of individuals and organisations who are involved in terrorist activities publicly available**[24]

Enable

- **Design simple models to aid public understanding and action**
  - Example: UK Model (Fig 8-2)
    - Cycle of terrorist attack: Target Selection through Exploitation
    - Counter approach: Deny, Detect, Deter
- **Provide instructions and platforms for reporting**
- **Encourage and support community social groups interested in safety and security (i.e., crime watch groups, disaster preparedness committees) (**Vol II, Ch 3, Sec 4)
- **Encourage public to voluntarily participate in defence against terror exercises**
  - Private individuals and companies are often willing to provide training venues
- **Establish Public/Private Partnerships**
  - **Example 1**: Danish SSP system: Local collaboration between schools, social services and police[25]
    - Organised on three levels
      - ✓ Political strategic level
      - ✓ Coordinating level (local authorities)
      - ✓ Implementing level (local professionals from schools, etc.)
  - **Example 2**: "New York City Police Department (NYPD) Shield" Programme[26]
    - Public-Private partnership designed to increase information training
    - Participating commercial enterprises receive the following:

[21] https://www.dhs.gov/see-something-say-something
[22] https://www.dhs.gov/see-something-say-something/take-challenge
[23] https://www.ict.org.il/Article/919/Creating%20a%20Citizenry%20Prepared%20for%20Terrorism%20Education,%20Media,%20and%20Public%20Awareness#gsc.tab=0
[24] https://www.government.nl/documents/reports/2016/01/15/national-terrorism-list
[25] https://ec.europa.eu/home-affairs/node/7488_en
[26] https://www.nypdshield.org/public/about.aspx

Enabling capability or action
✓ In-person intelligence and threat briefings conducted by CT Bureau and Intelligence Division personnel ✓ Informal conferrals with Patrol Borough CT Coordinators ✓ NYPD Website postings ▪ Shield Alert e-mail messages ▪ In exchange, enterprises agree to the following: ✓ Report suspicious behaviour as soon as possible. ✓ Speak with police officers when they are in the area ✓ Share perspective on security matters
 ***Figure 8.3 UK-ACT Awareness Programme***

8.15 **Intergovernmental Coherence.** In addition to the coordination-related measures discussed in Chapter 5, national governments must proactively encourage and require sub-national and municipal entities to acknowledge their responsibility to lead all phases of a whole-of-society defence against terrorism. This includes completing necessary training. Under some circumstances, the national government will need to provide or supplement the training. However, even if national resources are not required, coordination with the national government is important to ensure coherence across the whole-of-society.

- Table 8-8 presents a small example of the type of training the national government may wish to provide
- Where feasible, integrate members of the population into the training, either in support of officials or as role players

Table 8.7 Sample national/sub-national/municipal training programme

Case	Examples
US U.S. Dept. of Homeland Security (DHS) makes courses available to	**Resident Examples** • WMD Crime Scene Management for Emergency Responders (CSM) • Standardized Awareness Authorized Trainer Program (Train-the-Trainer) (SAAT)

Case	Examples
state or local responders. The training is completely funded by the national government at no cost to the individual or jurisdiction, to include meals and lodging.[27]	• Radiological Emergency Response Operations (RERO) • Incident Command System Curricula Train-the-Trainer • Managing Civil Actions in Threat Incidents (MCATI) Command • Command and WMD Response (CMD&R) • Hospital Emergency Response Training for Mass Casualty Incidents (HERT) • Healthcare Leadership and Administrative Decision Making (HCL) • Pandemic Influenza Planning and Preparedness (PIPP) • WMD Emergency Medical Services (EMS)
	Mobile Courses Examples • WMD Crime Scene Management for Emergency Responders (CSM) • Standardized Awareness Authorized Trainer Program (Train-the-Trainer) (SAAT) • Managing Civil Actions in Threat Incidents (MCATI)

Table 8.8 SOF's role in preparing society to defend against terrorism

➢ **Building counterterrorism capacity among members of the population, particularly cultural awareness and threat recognition training**
➢ **Guide and mentor private and civic sector integration into civil (law enforcement) CT training and exercises where legally permitted Language and biometric screening in support of law enforcement**
➢ **Support whole-of-society target analysis, including situational awareness and intelligence sharing (where permitted)**

8.16 Assessing the Risk of Terrorist Acts

- Chapter 11 presents the Comprehensive Risk Assessment (CRA) process in detail. This section focuses on a unique aspect of the planning process that applies specifically to assessing threats posed by terrorist acts. It is placed here for context and is best used in conjunction with Chapter 11.

- Adding the additional step of categorising potential terrorist targets when conducting the risk identification and analysis of the CRA will help planners recognise key private and civic stakeholders during the planning process.

[27] https://www.in.gov/dhs/2611.htm

Table 8.9 Sample terrorist target category chart

Target Category	Places where people congregate
Recreation	Stadiums, concert halls, entertainment venues, festivals, parks, markets, shopping malls, theatres, cinemas, clubs, restaurants, bars, cultural events, parades, pedestrian areas etc.
Commercial	Hotels, apartment buildings, office complexes, shops etc.
Public	Hospitals, medical centres, universities, schools, museums, libraries, etc.
Religious	Places of worship, religious events, etc.
Transportation	Train and subway stations, airports, bus and port terminals, transportations sites, etc.
Governmental	Town halls, ministries, official residences, monuments, landmarks governmental office complexes, etc.

Table 8.10 Considerations when identifying and analysing terror-related risks

Step	Considerations
Risk Identification	• **Learn from, but do not overemphasize past acts** o Terrorist tactics adapt and transform according to political and religious factors, perpetrator skills and available resources, available instructions and propaganda, etc. o The most recent events normally reveal the most relevant trends • **Do not limit analysis to intelligence and law enforcement resources** o There is an abundance of information available through academic and commercial sources o When dealing with transnational terrorist groups, examine trends across the group's geographic area of interest
Risk Analysis	• **When evaluating likelihood, consider the following questions**[28]

[28] Pg 93

	o Are there any indications of an imminent terrorist attack? o Does the potential target represent a religious/ethno-nationalist ideology that is against the political or religious agenda of active terrorist groups? o Is the target of symbolic or historical value? o What is the maximum attendance? o Are there any high profile events hosted that are attended by famous people and covered by the media? o Are there any trained security officials present? o How easily accessible are the targeted premises and by what means (car, motorcycle, foot, etc.)?

- After risk identification and risk analysis, planners will categorize targets using the following Vulnerability Assessment Nomenclature

Table 8.11 Sample Vulnerability Assessment Nomenclature[29]

Level	Description
Low vulnerability	The examined infrastructure or public space is equipped with adequate security countermeasures (controlled access, safeguards, perimeter protection etc.) to drive away potential aggressors and is unattractive as a potential target.
Moderate vulnerability	The examined infrastructure or public space may be equipped with some security countermeasures (no controlled access, some safeguards, partial perimeter protection etc.) and is well-known only at a local scale.
High vulnerability	The examined infrastructure or public space is characterized by inadequate security countermeasures, while it is well-known at a national scale.
Very high vulnerability	The examined infrastructure or public space is characterized by inadequate security countermeasures, while it is well-known at a global scale.

Table 8.12 Key Takeaways- Weaponised Information, Cyber Attacks, and Terrorism

Society's primary contribution when combatting the type of terrorism described here comes from the ability of individuals to recognise and possibly disrupt an attack, while incurring minimal risk

- A well-trained, well-educated public is also capable of minimising casualties if an attack does occur

From the perspective of comprehensive defence, the government's focus should be on establishing effective education and information programmes that will reach the whole-of- society

- Members of society should also be integrated into national and sub-national counterterrorism assessments, planning and exercises

[29] Pg 94-95

Chapter 9 Malicious Act: Armed Incursion

This chapter provides specific considerations for establishing a whole-of-society capability to defend against an armed incursion.

Section 1—Overview

9.1 The primary goal and greatest strength of comprehensive defence is the role it plays in resilience and deterrence. Nevertheless, from a whole-of-society perspective in particular, preparing for and responding to an armed incursion requires significant effort. For this reason, it also provides a useful framework for identifying the actions the government must take to enable the population to defend itself against a partial or total occupation.

9.2 This chapter uses the same approach as Chapter 8. Actions the nation would likely take in response to an armed incursion are presented along with considerations regarding society's potential role relative to each action. The references noted lead to sections within the handbook that contain further details as well as checklists for preparing the population to perform the functions described.

Table 9.1 Context for considering whole-of-society defence to armed incursion

The nation has been fully or partially occupied by force. The belligerent occupier has declared itself the governing authority and exerted its control over many critical functions. The occupied nation's legitimate government has either moved into exile or is operating clandestinely from within its occupied country. Under the described circumstances, the nation has the option to either fully submit to the occupying power or resist and re-establish its sovereignty and right to self-determination. Below assumes the people choose to resist.

9.3 **Armed Incursion.** There are several ways in which the incursion described above may unfold.

- Foreign military force breaches a nation's physical border and withdraws quickly (i.e., days or weeks)
- Foreign military force breaches a nation's physical border and remains to occupy part or all of the breached nation's territory
- Foreign power uses paramilitary or disguised forces to covertly invade and occupy a nation or open the way for an overt occupying force
- Some combination of each

9.4 **Indications and warnings.** In addition to potentially obvious troop movements, it is possible that the adversary took certain "hybrid" actions before the attack which, if recognised, would have indicated the enemy's intentions.

- Cyber attacks to compromise communications or defensive capabilities
- Weaponised information campaign
- Insertion of agents

- Seizing key buildings or infrastructure
- Incite political or civil unrest—phony referenda

9.5 **Desired State.** The 98% have the skills necessary to recognise an impending attack, survive, report and participate in a whole-of-society defence during the initial stages of an armed incursion

Table 9.2 Capabilities: Initial Incursion

Enabling Capability or Action	Reference
• Educate and train all members of society to survive an armed incursion* o Survive potentially lethal enemy actions o Evacuate occupied territory • Recognise and report suspicious activity, to include "hybrid" actions **Most of the skills are applicable in any type of emergency*	• Vol II, Ch. 5

Section 2—Legitimacy

9.6 **Perspectives**. Aside from protecting the population, the government's highest priority will be to maintain the state's legitimacy, which will be viewed from three related perspectives.[30] The first two perspectives are directly relevant to comprehensive defence.

- Maintaining a legitimately recognised international legal personality
- Maintaining the confidence of the population to represent the state
- Maintaining legitimacy needed to receive international support

9.7 **Maintaining the State.** In the first two examples in paragraph 3.3 the state is clearly engaged in international armed conflict.

- International laws and diplomacy will come to the fore as the two opposing powers seek to justify their positions among the global community of states.
- It will be in the defending nation's vital interest to ensure that its government remains intact, even if the official governing body displaces and operates in exile.
- Should the government cease to exist, the defending nation's international legal personality will be challenged, and the defending nation will be incapable of effectively representing itself (or its population) in international forums.

[30] It is important here not to confuse the state with the government. The state has four essential elements—Population, Territory, Government and Sovereignty. The government derives and exercises authority on behalf of the state. Furthermore, sovereignty is a characteristic of the state, not the government. This is important, because the government is not trying to defend itself. It is leading the defence of the state (aka country).

- The legitimacy of the armed forces will also be challenged, as the occupying power will likely declare itself the legitimate head of state and designate all opposing forces (i.e., the defending army, asymmetric defence component, home guard, etc.) to be terrorists or insurgents.
- During the Prepare Phase, accounting for the considerations listed in Table 9-3 will help set the conditions for the state to maintain its international legal personality in the event of an armed incursion
  - ✓ The government must plan for displacement or foreign exile and establish a legal framework ensuring its legitimacy
  - ✓ Mutual aid agreements with neighbouring states, regional powers, and allies as well as bilateral defence agreements must be made prior to conflict
  - ✓ The government must plan for a stay-behind leadership structure (shadow government), to assist in the conduct of resistance operations and provide governance to compete with the enemy's occupation regime, maintaining confidence that the legitimate government is still functioning

Table 9.3 Planning considerations for displacing government

Consideration	Explanation
Evacuation Plan	• How is evacuation initiated • By what means will officials travel • Travel alone or as a group(s) • Communication plan
International Agreements	• Important to establish in advance o With government that will host the exiled government o With allies and partners to reaffirm continued support and recognition
Communications plan	• Means to initiate exile order • Communications with host government • Communications back to occupied nation
Virtual diplomacy plan and means	• Secure back-up servers in place during preparation phase oEstablish treaty with nation that will host server to protect against breach/loss of sovereignty[31] oConsider operating from one of the nation's own embassies in a foreign state
Clear responsibilities for governing elements that remain behind	• What governing responsibilities will the exiled element have • What responsibilities and authority will the remain-behind element have • When, if at all, should the remain-behind element cooperate with the occupying force

[31] It is important to establish and maintain back-up servers well prior to any indications of an incursion. Using these servers should become a matter of routine. Note that some nations have laws that allow the government to access data under certain conditions. If the back-up servers are located in a state with such laws, the occupied nation's data may be at risk at all times

Command and control of Asymmetric Defence Component	• Pre-establish C2, to include shadow government o Imperative that the legitimate government direct all ADC actions o Ad hoc cells, which do not support the legitimate government will become a liability and will be used by the adversary to justify their actions

9.8 **Legitimacy in the eyes of the population.** Four factors will affect the government's ability to maintain popular legitimacy.

- Ability to reassure the people that the nation will survive and prevail
- Professional conduct by the nation's defence forces and governing officials
- The level of social and psychological resilience among the population
- The enemy's actions

Table 9.4 Key Point

The government's ability to maintain legitimacy on behalf of the state relies largely on comprehensive defence-related actions taken before the crisis

9.9 **Desired State.** Society capable and willing to contribute to the survival (i.e., sovereignty) of the state.

- All aspects of society's ability to support state and government legitimacy relate to actions taken during the comprehensive defence preparation phase.

Table 9.5 Enabling whole-of-society contribution to legitimacy

Enabling capability or action	Reference
Government in Exile • The government and military will almost certainly require support from the population to evacuate and establish a government in exile o Society's role should be included in national comprehensive defence plans	Vol II Ch. 4
Legitimate legal personality • Society should be made aware in advance that the government will function from abroad in the event of an incursion o The population may otherwise feel abandoned • Elements of the population should be prepared to support the government's movement into exile o Assist with transportation o Reconnoitre routes in advance of movement o Provide safe haven: i.e., safe house, hiding locations o Logistical support—food, water, etc. o Understand the national narrative and strategic communications approach	Vol II Ch. 3 & 4
Popular legitimacy • Establish cellular "shadow government" structure during peacetime • Pre-crisis investments in social and psychological resilience • Ability to identify misinformation o Adversary will try to use propaganda to undermine the government's legitimacy	Vol I Ch. 2 & 8

Section 3—Mobilising the Defence

9.10 **Considerations.** The military component of the nation's comprehensive defence forces will likely comprise three elements—standing armed forces, home guard and asymmetric defence component.

- When activated, some ADC members will need to move to a designated site, while others will remain in place
- The identities of key ADC members must be guarded, even during peacetime
- This security requirement complicates recall
  - ✓ Keep the force informed and notify the ADC of potential activation as early as possible
  - ✓ Security becomes increasingly difficult as the crisis develops
  - ✓ It is critical to have redundant means of secure communications
    - The fact that the ADC is being activated is not necessarily secret, as this is expected. People within the ADC and their families is what is being protected.
    - Communication need not be point to point
      - Song on the radio
      - Particular flag or symbol at pre-designated location

Table 9.6 Key Point

It is important to develop secure, redundant means of communications for activating the Asymmetric Defence Component

Section 4—Command and Control

9.11 **Comprehensive Defence Command and Control (C2) Methods.** Faced with the given situation, the nation will need to simultaneously employ three methods of command and control

Military Style	• For professional standing forces (including reserves) • High trust • Strong control levers • Good survivability • Hierarchical o Orders driven o Compliance expected
Interagency	• Some home guard elements • Private and civic sector supporters • Medium trust o Can achieve high trust through relationships and procedures • Some control levers • Good survivability • Synchronizing, not commanding

Compartmented	• ADC and elements of home guard • Pockets of trust • Some control levers • Survivability varies • Command by intent • Trading security/secrecy for control

9.12 Comprehensive Defence C2 Challenges

Legitimacy of displaced government	• Are we revolutionary insurgents or a professional defence force? o If the government is illegitimate, the force it commands is illegitimate
Vertical vs. Decentralised structures	• Hierarchical control and trust vs. Network security
Lack of architecture	• Interagency architecture not set up to accommodate whole-of-society collaboration
Three sets of laws to follow	• Occupier laws • National laws • International laws
Operational Security (OPSEC)	• Collaborators & infiltrators • Poor practices
Resources	• How to get money
Information campaign	• Occupier probably controls media

9.13 **Desired State** (C2). Nation capable of providing command and control of defence and/or emergency response forces during peace, crisis or war

Enabling capability or action	Ref
• **Build trust through preparation** o Establish cellular structure during peacetime ▪ Fill core positions o Interagency and compartmented styles work well when trained and rehearsed ▪ Teams naturally develop reliable procedures and SOPs	Ch. 5
• **Train as cells** o Becomes very secure with adequate training o Never break security/secrecy o Cellular structure resilient if “critical nodes” not identified	
• **Training and education will reduce uncertainty and mitigate doubt** o Doubt undermines legitimacy/confidence in government	Ch. 6
• **Simulate realistic strategic conditions during training** o Leaders use table top exercises and to draw out legal and financial considerations	
• **Incorporate legal training and discussions into all training** o Whole-of-society must understand their rights, protections and responsibilities when contributing to comprehensive defence o Involve private sector in resource-related discussions	

Enabling capability or action	Ref
• **Harden society against weaponised information** • **Expand interagency architecture to accommodate all stakeholders** o Leave in place at all times o Use during non-crisis to support collaboration and training	Ch. 14

Section 5—Comprehensive Defence Infrastructure

9.14 **Physical Infrastructure.** [32] Special consideration should need to be given to physical infrastructure requirements.

- ☐ Command posts
  - ✓ Covered routes in and out
  - ✓ Clandestine communications
- ☐ Training facilities
  - ✓ Recruitment and training continue
- ☐ Logistics storage facilities (Vol II, Ch. 5)
- ☐ Means of transport and movement

Table 9.7 Key Point

Secure human infrastructure (people) provides secure physical infrastructure

Section 6—Comprehensive Defence Operations.

9.15 Defensive operations will take one of three forms

- ☐ Regular armed forces supported by ADC and home guard
  - ✓ ADC and home guard used primarily for the following functions
    - Logistics
    - Information
  - ✓ Blended force
    - ADC integrated into armed forces
  - ✓ ADC and home guard only
    - Regular force fully committed in a different location
    - Impractical for the situation
    - Nation does not maintain a standing armed force (small state in particular)
- ☐ Approach can change based on situation and plans

9.16 **Asymmetric Defence Component employment**

- ☐ ADC capable of performing a range of support, violent and non-violent missions
- ☐ ADC structure and activity will remain clandestine during peacetime and conflict

[32] https://weburbanist.com/2016/01/12/under-cover-secret-swiss-military-bunkers-hide-in-plain-sight/

9.17 **Desired State.** Society is prepared to conduct and/or support comprehensive defence operations

Table 9.8 Society's support to comprehensive defence operations

Enabling capability or action	Ref
Common Skills • Conduct secure communications • Link up with individuals and units • Operate in occupied territory • Blend in with the population	Vol II, Ch. 5
Non-violent resistance • Concepts and techniques of nonviolent resistance	
Logistical support • Construct a cache site construction • Provide secure training facilities	
Medical support • Provide tactical combat casualty care • Provide clandestine medical care	
Reporting • Describe terrain • Describe people • Describe equipment	
Blended operations • Help control supporting fires (Joint Fires Observer) • Conduct cellular operations • Specialty Skills	Vol II Ch. 4

Table 9.9 Key Take Aways--Armed Incursion

- **For most nations, an armed incursion is the least likely but most dangerous malicious act imaginable**
- **It is also the one which, from a whole-of-society perspective, requires the greatest amount of preparation**
- **Preparing society to defend itself against an armed attack further reduces the likelihood that such an event will occur**
- **Moreover, the actions undertaken to enable the population to respond to an armed incursion will increase the nation's resilience against threatening natural and accidental events as well**

Chapter 10 –Role of Armed Forces in Comprehensive Defence

This chapter presents considerations for the military's role in comprehensive defence.

Section 1—Overview

10.1 The militaries of most nations possess massive capacities, which under a traditional defence construct are focused solely on preventing, preparing for or responding to crisis or conflict. There are normally provisions, even under the traditional approach, for the military support law enforcement or disaster response agencies. However, in general, determining the military's role in whole-of-society approaches to public safety and security is not an intuitive and, therefore, warrants particular attention.

10.2 Similarly, nations' Special Operations Forces (SOF) normally possess unique capabilities that are seldom considered in context of comprehensive defence.

Section 2—Governing Factors

10.3 **Governing factors**. The military's role in comprehensive defence will vary according to four factors

- Type of emergency (natural, accidental, malicious),
- Operating domain (air, land, sea, cyber)
- In the case of an armed incursion, the method of response (conventional, irregular/asymmetric, blended)
  - ✓ If the nation established an asymmetric defence component, the command relationship between that component and the armed forces will influence the role the nation assigns to its military
- Law and policy. No matter what functions are assigned, when employed within a comprehensive defence construct, the military will operate alongside, or integrated with, non-military governmental organisations and members of the private and civic sectors
  - ✓ Develop the necessary legal and policy frameworks well in advance of any event that will call for a whole-of-society response (Ch. 11)
- Readiness. Given the enormity of its capacities and capabilities, there may be a temptation to overtask the military or assign tasks that detract from readiness
  - ✓ Always consider the impact the comprehensive defence roles assigned to the military will have on its ability to deter and defend against malicious acts

Section 3—Considerations

10.4 While many of the considerations listed below also apply to malicious acts, the list is designed to primarily to highlight the potential military roles relative to natural or accidental events.

Table 10.1 Potential Military Roles in Preparation and Response to Non-Malicious Act

Function	Considerations
Logistics	• **Ability to stockpile, transport and distribute large amounts of supplies, to include humanitarian aid** • **Movement control, to include guiding movement of displaced persons** • **Temporary shelter: i.e., constructing camps** • **Maintenance support** • **Medical support**
Planning	• **Planning capability and capacity** o Military leaders at all levels are well versed in planning and military planning procedures may be easily adapted to serve non-military purposes o Equally applicable to long-range, strategic planning and immediate crisis response requirements • **Analytical capability and capacity** o Discrete subset of planning capacity
Coordination	• **Military command and control procedures and architecture may be used to supplement or frame non-military response** • **Ability to organise and lead multi-functional teams**
Operations	• **Search and rescue capabilities** • **Manpower** o Fire fighting o General disaster relief tasks (e.g., filling sandbags) • **Crowd control in support of civilian agencies (i.e., law enforcement, border guard services, etc.)** • **Strategic communications** o Military public affairs and information support elements may help develop and transmit strategic communications messages • **Cyber Defence** o Military tends to have significant cyber defence capability ▪ Must be synched across society ▪ May be able to augment other sectors • **Evidence collection** o Military “sensitive site exploitation (SSE)” procedures and capacities may be adapted to evidence collection and forensic analysis
Training	• **Allowing non-military organisations to train on military facilities increases cohesion and reduces cost** o Consider and mitigate potential impacts on military readiness

	▪ Prioritising access to training facilities ▪ Security o Consider designing multi-agency/multi-purpose facilities • **Military training and exercise design procedures can be easily adapted to serve non-military purposes**

10.5 The following list offers considerations for potential military roles in response to armed incursion.

Table 10.2 Potential Military Roles in Preparation and Response to Malicious Acts

Function	Considerations
Relationships	• **When responding to events other than armed incursions, military comprehensive defence responsibilities will almost always be performed in support of civilian agencies** • **When responding to armed incursions, the military will likely perform a leading role in parts or all of the response** o Alternatively, lead role may also be assigned to Ministry of Interior/security services • **Relationship with Asymmetric Defence Component will depend on response method and force design** • **Response methods** o Symmetrical o Asymmetric o Blended • **Force design examples** • Supported/supporting • Home guard (and/or ADC) integrated into military • Home guard (and/or ADC) and military separate—MOI lead
Security	• **Implement counter network analysis/contact tracing procedures to protect ADC member identities** o Example: Adversary identifies ADC casualty; associates casualty with other acquaintances and family members
Capability Integration	• **Implement plans and procedures for integrating civilian capabilities** o **Navy/Maritime Domain** ▪ Commercial and recreational seafarers o **Air Force/Air Domain** ▪ Plane watchers ▪ Commercial and recreational pilots ▪ Drone enthusiasts o **Army/Land Domain** ▪ Geo-caching ▪ Dog trainers and handlers ▪ Tracking enthusiasts o **Space Domain** ▪ Amateur satellite trackers

Recruitment and Training	• **Recruitment and training of military, home guard and ADC personnel does not cease in event of armed incursion**

Section 4—SOF's Role in Comprehensive Defence

10.6 Before considering SOF's role in comprehensive defence, it is useful to first identify the institutional attributes and characteristics that make SOF unique relative to the nation's conventional forces.

- SOF Attributes. Though definitions of special operations and SOF vary by nation, most relevant to comprehensive defence is a near universal reference to the pursuit of *strategic effects* within *politically sensitive* environments, which leads to the following traits:
  - ✓ Highly adaptable
  - ✓ Acute appreciation for culture
  - ✓ Achieves missions by working "by, with and through" the populations in which they operate
  - ✓ Commonly required to produce strategic effects in politically sensitive environments
  - ✓ Commonly and readily interface with non-MOD organisations, governmental and non-governmental alike

- SOF's Missions. SOF missions vary by nation. However, SOF among most nations commonly perform the following mission sets[33]:
  - ✓ Direct Action— short duration strikes and other small scale offensive operations principally undertaken to seize, destroy, capture, recover, or inflict damage on designated personnel or material
  - ✓ Special Reconnaissance—Actions conducted in sensitive environments to collect or verify information of strategic or operational significance
  - ✓ Military Assistance—Training, educating, advising and supporting partners (most often in the partner's area of responsibility)

- Categories of SOF. Forces executing the special operations missions noted above fall within one of two categories (Fig. 10.1).
  - Direct SOF
    - o Effects focused directly on the adversary
    - o Typically conduct DA & SR
  - Force Multiplier SOF
    - o Enables effects to be delivered by, in collaboration with or through the population
      - ▪ Typically conduct MA with home guard, asymmetric defence component and/or conventional forces
      - ▪ May lead and/or accompany ADC during operations

[33] https://www.nato-pa.int/document/2018-special-operations-forces-moon-report-169-dscfc-18-e-rev1-fin

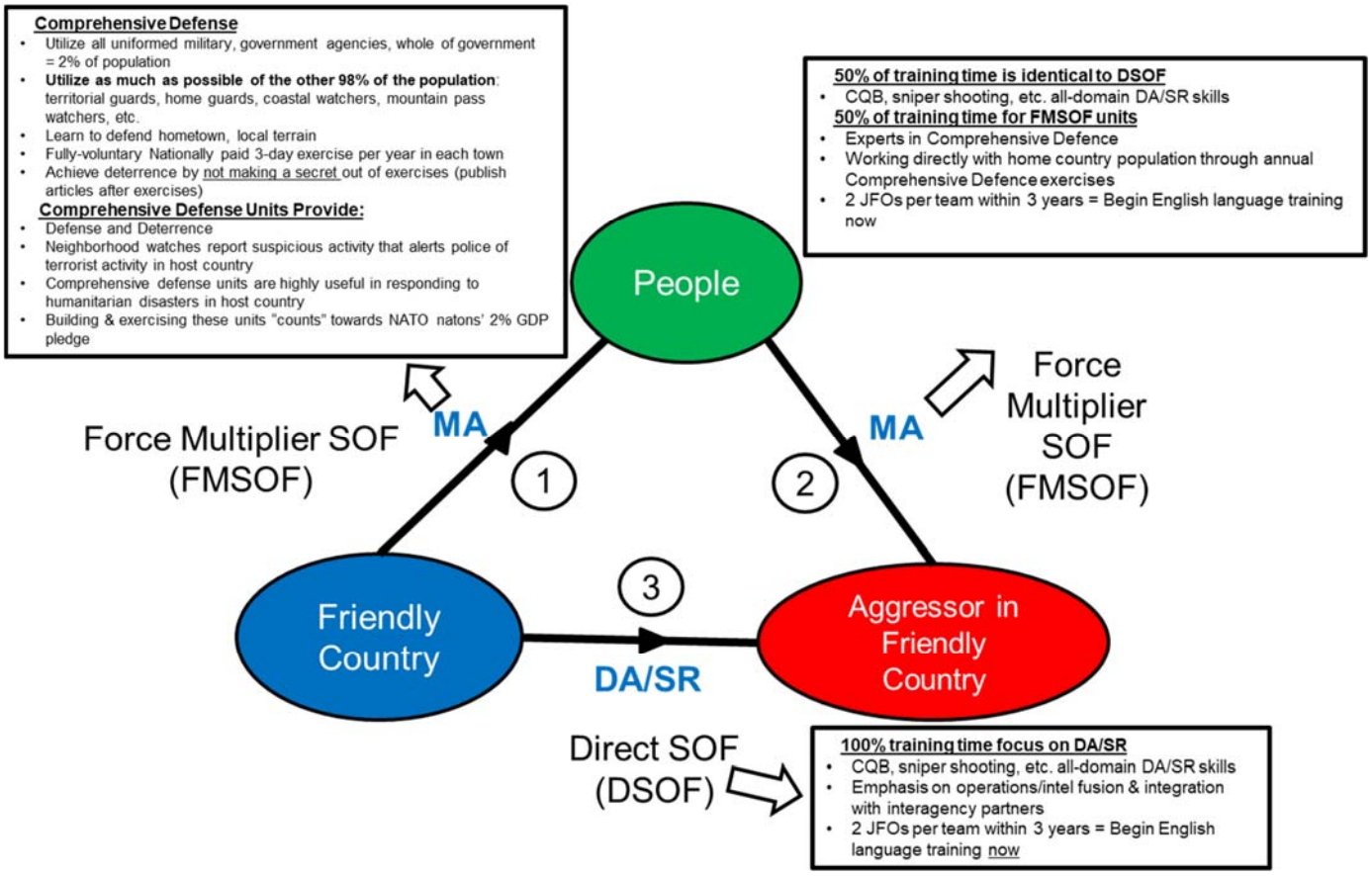


Figure 10.1 SOF as Force Multiplier

10.7 Potential SOF Tasks in Comprehensive defence

- Liaison functions with private and civic sector organisations
- Advising and assisting non-military government agencies
- Conducting critical infrastructure assessments
  - ✓ Looking for weaknesses that could be exploited by the enemy
- Training conventional force in military assistance
  - ✓ Conventional force then trains assigned home guard elements
- Recruiting, assessing and training ADC elements
- Leading ADC elements

10.8 **Special considerations for SOF employment**. SOF are inherently comprehensive in their structure. Because of their unique expertise and the high regard in which SOF are often held, they may at times be placed in position to lead a relatively large portion of a comprehensive defence effort

- When placed as team captains, SOF must be trained to demonstrate the requisite leadership skills of respect, cooperation, and motivation with their other comprehensive partners

- SOF should include other members of the public, private, and civic sectors in all planning efforts
  - ✓ This is particularly true in asymmetric defence operations

Table 10.3 Take Aways—Military's Role

➢ Military is capable of contributing to several aspects of comprehensive defence o Careful planning and analysis are necessary to ensure military is employed wisely ➢ SOF has unique capabilities that are particularly relevant to comprehensive defence o Force multiplier role is often most applicable and easily overlooked

Chapter 11 —Legal Considerations

Section 1—General considerations. Comprehensive defence must be supported by a distinct set of laws and policies, which are designed to allow necessary whole of society cooperation while safeguarding civil liberties and protecting sensitive security, proprietary and law enforcement information.

11.1 **Interagency Cooperation.** All nations have laws and policies that enable and/or limit cooperation between various government organisations.

- Laws designed specifically to limit or enable cooperation
- Laws that inadvertently limit or enable cooperation; i.e., laws that effectively prohibit cooperation through funding rules; laws that define agency structures; laws that specify rules for sharing and safeguarding information

11.2 **Private and Civic Participation.** National laws are normally constructed with an eye toward limiting private and civic exposure to disaster response, defence, and security matters, rather than enabling direct private/civic participation. Consequently, existing laws may inhibit whole of society approaches. Consideration should be given to protecting the liability of private parties assisting in government lead comprehensive defence activities.

- Countering Hybrid Threats. Policies and procedures will need to be established to ensure civilians who support the government in countering hybrid threats or crisis response efforts receive adequate legal protections.
- Armed Incursion. Policies and procedures will need to be established to ensure civilians who support Comprehensive Defence, in the event of an armed incursion, are properly categorised to ensure they receive adequate legal protections under the Geneva Conventions; i.e., participant in *levee en masse*.
- Nations should clearly delineate which civilians will serve in a combat or non-combatant status. Civilians who become part of an armed citizen defence corps will be considered combatants and may be targeted at all times; e.g., a civilian who drives a truck with military supplies may be targeted during the delivery but not once the task is complete. However, the driver can still be apprehended and detained for posing a security risk, even after the fact. Governments should ensure all civilians taking part in comprehensive defence understand these risks.
- Failure to adequately address this consideration will place inhabitants at risk of being treated as spies, insurgents or some other non-desirable category.

11.3 **Legitimacy.**

- Domestic. In addition to the need to safeguard civil liberties, nations must consider how comprehensive defence-related laws and policies impact Social and Psychological resilience. Perceptions of government overreach will undermine national efforts to encourage private and civic participation in Comprehensive Defence.
- International. Particularly as it applies to comprehensive defence against a malicious actor, international support is essential. Actions which violate international laws and

norms will risk losing external support, to include practical assistance; i.e., "funding, training, equipment, direct participation, planned conventional military support by allies and partners or other assistance rendered by external partners."[34] Additionally, international law may subject individuals, nations or national leaders to adjudication at an international or military tribunal. Nations must, therefore, ensure all Comprehensive Defence practices respect human rights and are guided by applicable treaties, International Humanitarian Law (IHL), Law of Armed Conflict (LOAC), and other pertinent international customs and norms.

[34] Resistance Operating Concept (ROC). Swedish Defence University, 2019. p85

Table 11.1 Legal Considerations

Function	Consideration	References
Interagency Cooperation	• Laws and policies support information sharing among agencies, while protecting individual privacy rights • Laws and polices support collaborative planning among agencies • Laws and policies governing funding and procurement allow agencies to share equipment • Laws and policies facilitate supporting/supported arrangements; i.e., military support to law enforcement; intelligence services support to domestic military operations, etc.	
Civic Participation	• **Laws and policies governing the formation of volunteer emergency response organisations and their ability to contribute to crisis prevention and response** o Training and equipping requirements o Funding requirements and sources o SOPs o Employment rights (i.e., protect against job loss when activated as a volunteer emergency responder) o Compensation and/or medical treatment if injured while performing voluntary emergency response duties • **Laws governing conscription, to include conscription into civil service** • **Laws governing the status of home guard organisations and their relationship with the government during all phases of Comprehensive Defence (Preparation, Response and Recovery)** • **Policies and procedures to reinforce the legal status of individuals who participate in Comprehensive Defence in the event of armed incursion** oMember of armed forces oCivilian participant in a *levée en masse* • **Laws and policies governing reintegration of civilians upon cessation of hostilities**	• ROC, pg 93-95 • 1977 Additional Protocols (AP) of the Geneva Conventions (GC) oAP I (Art 51) oAPI (Art 43(1)) oAP I (Art 43(3)) (FN 166, 67, 68) o(GC III Art 4, Par A (1) (2) (3) (6))
Continuity of Government	• **Plans and policies accounting for laws applicable to lawful (exiled) government**	

Function	Consideration	References
	o If a government in exile is planned, consider establishing laws that invalidate decisions and guidance issued by ministries physically located within occupied territory o Exiled government should work with international community to create a post-conflict system to fairly adjudicate LOAC violations of occupying forces.	

Chapter 12 Stakeholder Mapping

This chapter offers a process for determining stakeholder interest and influence relative to comprehensive defence.

Section 1—Overview

12.1 In general, members of the private and civic sectors (the 98%) cannot be compelled to perform active roles in comprehensive defence. Therefore, governments must take deliberate steps to create communities of practice (COPs) and communities of action (COAs) that include members of society who are willing to contribute to disaster response, defence and security. The first of these deliberate steps is to identify and map stakeholders based on their interests and influence relative to comprehensive defence.

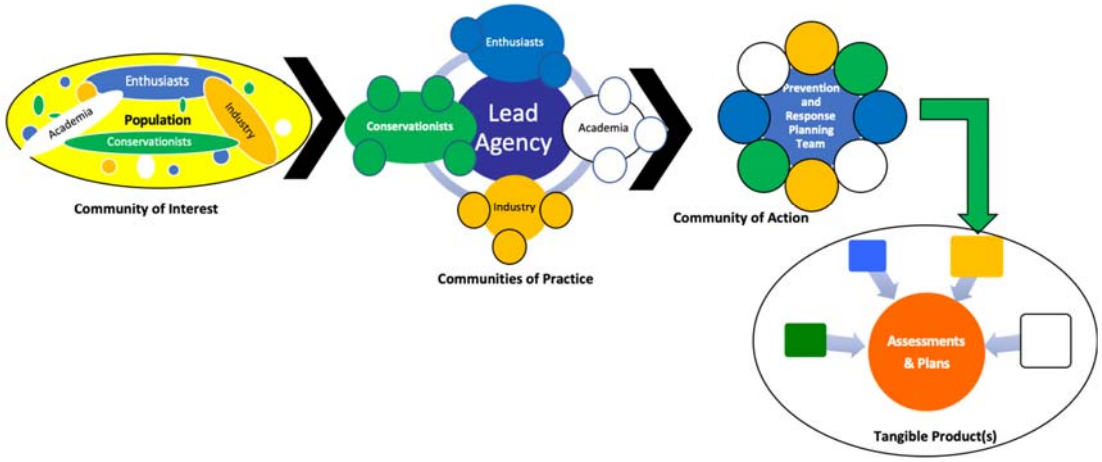


Figure 12.1

Section 2—Stakeholder Communities

12.2 **Communities of Interest (COIs)** are formal or informal groups composed of persons who regularly apply some level of attention to a common subject.

- Members are normally linked through the physical or virtual platform(s) they use to share information across the group
  - ✓ Internet Forums
  - ✓ Speaking engagements, etc.
- For example, numerous maritime-related communities of interest exist
- Maritime COI focus areas range from conservation to recreational and commercial fishing

12.3 **Communities of Practice (COPs)** are subsets of COIs.

- COPs produce physical or intellectual content related to the COI to which they belong
- Coastwatch Europe, whose members produce surveys on such things as marine litter and water quality is an example of a COP[35]

12.4 **Communities of Action (COAs)** are also subsets of COIs, and most members belong to one or more COP as well.

- COAs perform specific activities relevant to their associated communities
- For instance, several nations form COPs in support of a whole-of-society maritime early warning network, led by the MOI or MOD, and comprising governmental and non-governmental entities; i.e., fishing clubs, etc.

Section 3—Process

12.5 As illustrated in figure 12.1, constructing the comprehensive defence network entails drawing from communities of interest (COIs) to form a pool of subject matter experts and practitioners committed to contributing to the nation's resilience.

12.6 Because participation is voluntary and driven largely by personal interests, the level and nature of commitment and contributions will vary per participant and group.

12.7 The following six-step process and accompanying example will help those charged with creating or integrating COPs and COAs increase the chances of forming groups whose members will most assuredly contribute to the nation's interest.

- Steps
  - ✓ Step 1. Determine the purpose of the group being built
  - ✓ Step 2. Identify related COIs
  - ✓ Step 3. Identify related COPs
  - ✓ Step 4. Identify related COAs
  - ✓ Step 5. Analyse groups and their members to determine whether and how to engage
    - Power
    - Interest
  - ✓ Step 6. Engage groups and/or potential members to achieve one of the following outcomes
    - Advocate
    - Participate
    - Enable others to participate
    - Remain neutral (do not inhibit or obstruct)

[35] http://coastwatch.org/europe/international/ Coastwatch Europe (CWE) is an international network of environmental groups, universities and other educational institutions, who in turn work with local groups and individuals around the coast of Europe. CWE primarily protects wetlands by raising public awareness of their value and demonstrating practical ways to save them. Coastwatch Europe has participated at hundreds of events since the 1980's and published several dozen articles, scientific papers and books.

Section 4—Notional Example

12.8 In order to demonstrate comprehensive defence's broad applicability, the following example is not directly related to malicious acts. However, the stakeholder analysis process will be the same, regardless of the anticipated threat(s).

Table 12.1 Sample stakeholder communities

Purpose	Related COIs	Related COPs	Assessment and planning team (COA) members
Fire prevention, detection and response	• Outdoor adventurists • Conservationists • Industry o Lumber o Paper	• Clubs -Hunting -Fishing -Wildlife observation	• Local/regional fire & rescue • Volunteer fire • Volunteer rescue

12.9 **Step 1—Determine Purpose**.

- Per Table 12.2, a COA is being created to produce assessments and plans in support of forest fire prevention and response
  - ✓ The assessments and plans produced will be incorporated into the nation's Comprehensive Defence Plan

12.10 **Step 2-4—Identify related COIs, COPs and COAs**

- Individuals may be members of more than one COI and also belong to one or more COP and/or COA.
  - ✓ Outdoor adventure groups
  - ✓ Conservationists
  - ✓ Industry
    - ▪ Lumber
    - ▪ Paper
- COPs may routinely produce useful data, such as environmental conditions, backcountry access routes, hazards, etc.
- COAs differ from COPs in that COAs are designed to perform specific tasks. Possible examples follow.
  - ✓ Local/regional fire and rescue services
  - ✓ Volunteer fire
  - ✓ Volunteer rescue

12.11 **Step 5-6—Analyse Groups and Members and Engage Groups/Members**

- After identifying and mapping the community(ies), groups and key group members (i.e., stakeholders) each stakeholder is analysed according to the following categories listed in Tables 12.2 and 12.3, and engaged accordingly:

Table 12.2 Stakeholder Influence Rating

Rating	Definition
5—Very High	Stakeholder can direct (or have a massive impact on) the course of the project (i.e., COP or COA mission)
4—High	Stakeholder can have a major impact on the project's schedule and/or budget, and/or a minor impact on the project's scope
3—Moderate	Stakeholder can have a minor impact on projects schedule and/or budget
2—Low	Stakeholder cannot impact the project, but may know (or have access to) someone who can
1—Very Low	Stakeholder cannot directly impact the project

Table 12.3 Stakeholder Interest Rating

Rating	Definition
5—High positive	Stakeholder is highly supportive of the project and its benefits and will be angry if the project fails
4—Positive	Stakeholder sees benefit to self or others in the project and will be disappointed if the project fails
3—Moderate	If asked, this stakeholder would probably prefer the project succeeds, but does not feel strongly either way
2—Negative	If asked, this stakeholder would probably prefer the project didn't continue, but does not feel strongly either way
1—Low negative	This stakeholder is openly hostile to the project and its intended outcomes and will be vindicated if the project ends early

- The results can be quantitatively aggregated to inform an engagement strategy per the definitions and method contained in Tables 12.4 and 12.5.

Table 12.4 Stakeholder Engagement Strategy Definitions

Approach	Definitions
Monitor	Track stakeholder's commentary in traditional and social media to see if their level of interest (or access to influence) changes
Inform	Provide stakeholder with relevant, high-level information about the project at regular intervals/milestones
Consult	Obtain stakeholder's feedback on project decisions that are relevant to them
Involve	Rely on stakeholder's expert advice when making decisions about the project
Collaborate	Partner with stakeholder to develop alternatives and arrive at solutions that are acceptable to the collaboration group
Empower	Authorise stakeholder to make specific decisions about the project

Table 12.5 Influence-Interest combined score

		Interest				
		1	2	3	4	5
Influence	5	Consult	Involve	Collaborate	Empower	Empower
	4	Inform	Consult	Involve	Collaborate	Empower
	3	Inform	Consult	Consult	Involve	Collaborate
	2	Monitor	Inform	Consult	Consult	Involve
	1	Monitor	Monitor	Inform	Inform	Consult

12.12 Sustaining the Community

- The Comprehensive Defence Network cannot be "managed" in the same manner that a government organisation would be led and administered.
  - ✓ Most network organisations (COIs, COPs and COAs) function independent of the government
  - ✓ Many have no specific charter
  - ✓ Some will be suspicious of government intentions
- Under no circumstances should the government attempt to manipulate or compel participation from any group or individual
  - ✓ The network members do not serve the government.
    - The government enables the network members to contribute to their own safety and security
  - ✓ The government should recognise and incentivise participation where appropriate, while respecting the desire of any network members who may prefer to remain anonymous

Table 12.6 Key Take Aways--Stakeholder mapping

- **Stakeholder mapping is an indispensable step in all stages of comprehensive defence planning, beginning with concept development**
- **After implementing comprehensive defence, stakeholder mapping remains important for maintaining communities that comprise the nation's whole-of-society defence network**

Intentionally blank

Chapter 13 Concurrence

This chapter offers actions the government can take to gain broad, whole-of-society concurrence for transitioning to comprehensive defence and keeping the public informed after the initial implementation process is complete.

Section 1—Overview

13.1 **Public support.** Chapters 2-11 detailed considerations for increasing the nation's resilience through comprehensive defence. Discussions were centred on enabling members of society to participate in government-led resilience and response efforts, either individually or as part of a group. However, it should be noted that the idea for adopting comprehensive defence does not normally come from the 98%. While the benefits will be clear to defence, security and emergency response professionals, they will be less apparent to many members of society who will be asked to contribute personal resources and commit making sacrifices that they previously had no reason to consider. Thus, it impossible to implement comprehensive defence without explicit public support.

Table 13.1 Concurrence Lessons Learned

- Officials will need to gain society's concurrence throughout the implementation process
- Seldom will concurrence come in the form of a public "yes" or "no"
  - Yes/no will come from the legislative and legal processes
  - Most public statements will come in the form of action or inaction
- If no permission is needed, do not ask, but still inform
- The need for concurrence should be factored into planning timelines
- Many of the same methods used to gain concurrence will be used to provide information and education after implementation is complete

13.2 **Communication**. Communication will be the principal vehicle for gaining stakeholder concurrence and maintaining support across the society. A comprehensive defence communications programme (or line of effort) should comprise two elements:

- Information campaigns are designed to inform stakeholders of a particular aspect of comprehensive defence
  - Initial implementation
  - Change
  - Upcoming event, such as national training
- Institutionalised process designed to keep stakeholders aware of progress and developments

13.3 **Principles**. A comprehensive defence communications programme should be guided by the following principles.

- Always communicate to truth—any form of dishonesty or lack of transparency will undermine public trust and national resilience
- All communications should be two-way—comprehensive defence is based on collaboration, which requires two-way communications
- Perception matters—communication should never appear to be part of an indoctrination or influence campaign

Section 2—Information Campaign

13.4 The remainder of this chapter will provide considerations for developing an information campaign to support the implementation of comprehensive defence. Once complete, the information campaign should be merged into an enduring comprehensive defence public awareness programme.

Information Campaign Steps
1. Concept development
2. Stakeholder mapping
3. Initial consultations
4. Adjust concept
5. Conduct testing
6. Conduct campaign
7. Collect feedback

- The campaign objective is to ensure, as best as possible, that key stakeholders will support the nation's transition to comprehensive defence.
- A secondary objective is for those who do not directly support the transition to at least be comfortable enough with the initiative that they do not actively interfere with its implementation.

13.5 **Concept Development**. Prior to initial consultations, it will be necessary to develop the concept that will form the core of the information campaign.

13.6 The concept is not a detailed plan. It is a short description of the approach as it specifically applies to the nation.

13.7 Involve key stakeholders when developing the concept. There are two common methods for doing this.

- Stakeholders are part of the concept development team
- Stakeholders are included as members of an editing team that reviews the concept and provides input as it is developed

13.8 At a minimum, the concept should contain the following:

Table 13.2 Recommended information campaign contents

Topic	Key points
Key characteristics of comprehensive defence	• Overview of comprehensive defence framework • Encourages and enables whole of society participation • Focuses on making society more resilient • Broad calculation of cost implications (more or less public spending?)
Why change	• Threats to the nation have evolved • Through resilience, the nation is better able to prevent/deter, respond to, and recover from threats and emergencies • Reduces redundancy
What changes for members of society	• Increased individual resilience • More capable of contributing to safety and security • Education
Key implementation steps, per examples below	• Gain consensus • Educate • Organise • Develop human infrastructure

13.9 It is important to bear in mind that the concept will face demanding public scrutiny. Moreover, it is not unrealistic to imagine that a potential adversarial nation would use hybrid tactics to generate strong domestic opposition (see Chapter 2).

13.10 Therefore, initial consultations should be used, in part, to identify concerns that various stakeholders may express during the information campaign.

- Consultations are in addition to the collaborative method used to develop the concept.
- Table 4-3 describes potential issues regarding the asymmetric defence component (aka resistance force) within the comprehensive defence model, along with possible responses.

Table 13.3 Potential issues and considerations regarding asymmetric defence component

Potential Concern	Considerations
Planning to use this approach is **planning for failure**	• Asymmetric defence is only a response to failure when it is *not* planned and prepared prior to hostilities. • Otherwise, it is a deliberately constructed approach to national defence and serves as a strong deterrent to potential aggression. • Members of society who volunteer to join the asymmetric defence component members are professionally trained and governed by laws established to ensure appropriate oversight • An increasing number of nations are integrating the approach into their national defence plans for the same reasons being proposed here.

Potential Concern	Considerations
Home guard and asymmetric defence **militarizes society**	• There is a misconception that whole-of-society defence is merely a matter of arming all members of society so they can directly oppose the enemy should the country be invaded. • The first priority of comprehensive defence is to enable every member of society to develop the knowledge and skills necessary to survive in the event of crisis or war. • Next, home guard structures enable every member of society to defend their nation by performing a meaningful function of their choosing. The vast majority of functions do not involve bearing arms or engaging in direct combat.
Teaching society how to evict an occupying power **threatens democracy**, as the same capability can be used to overthrow the nation's current, legitimately elected government	• When deliberately implemented, home guard and asymmetric defence components are not rogue elements. They are integral elements of the nation's defence and security forces. o As the home guard and asymmetric defence component are developed, the nation crafts laws and policies to govern the force's employment, in keeping with the norms and standards of a free and open society. o Just as with traditional military service, the result is a more civically aware and responsible member of society. o The social and psychological pillar within the comprehensive defence framework further reinforces social harmony and civic responsibility. o The ADC's cellular structure inhibits mobilisation without the government-enabled coordination

13.11 **Stakeholder mapping** (see Chapter 10). Stakeholder analysis and mapping will need to be repeated continually throughout the consensus building process, beginning at concept development. It is useful to classify stakeholders according to their unique interests or functions. The analysis should include consideration for various sub-groups within each sector.

- Below are general considerations for each major sector. Along with the results of stakeholder mapping, these points should be considered during initial consultations and factored into the communications messaging.

Table 13.4 Stakeholder considerations

Sector	Key Points
Civic Sector. The civic sector is the most diverse and the most influential of the three groups. Ultimately, the civic sector will decide what course the nation will follow. They can communicate their position explicitly, through various formal mechanisms, or implicitly by demonstrating disinterest. If they do either of those two things, efforts to implement comprehensive defence will fail.	• Potential benefits o Increased resilience results in increased safety and security o Greater civic sector oversight of government actions o Greater ability to exercise right to protect the nation • Future collaboration points o Developing comprehensive defence education programmes (see Chapter 6) o Formation of home guard

Not only must the population approve, they must also commit to participating.	o Formation of ADC
Private Sector Opinions and interests will vary widely among members of the private sector. Messages cannot be tailored to every company, or even every type of company, but as many interests as possible should be accounted for when seeking support.	• Potential benefits • Brand recognition • Increased consumer loyalty based on respect for company's contributions o Likely future collaboration points • Determining private sector responsibilities for providing essential goods and services during an emergency, to include laws to compel certain actions o Cyber o Electricity, water, etc. o Logistics; i.e., transportation, construction, storage o Medical supplies • Implications of partial foreign ownership and influence over essential goods and services[36] • Lifelong learning programmes • Methods of integrating comprehensive defence into safety programmes • Formation of home guard • Formation of ADC
Public Sector It is easy to overlook government stakeholders. However, those responsible for managing implementation should not presume full understanding and support from across the public sector. Organisations and individuals that either do not agree with the approach or do not understand the concept may impede implementation.	• Implementation will require effort from all agencies; however, once implemented, all agencies benefit • Some structures and processes will need to change o Modify and expand government's coordination architecture and methods to enable whole-of-society collaboration o Integrate emergency response and national defence assessment and planning processes into a single procedure (see Chapter 10-11) • Establish legal frameworks • Adapt resourcing processes o Comprehensive defence expenditures will present new methods for calculating defence spending

13.12 **Initial consultations.** Conducting initial consultations with key members from each stakeholder community prior to conducting the information campaign will increase the chances that the campaign will provide the right information, in the right format, via the right platforms, in order to gain the desired support.

[36] The challenges many nations faced when trying to acquire medical supplies and equipment during the beginning of the 2020 COVID pandemic provides a recent example

- At a minimum, consultations should cover the following:
  - ✓ Review and gather feedback on concept
  - ✓ Gather perspectives on stakeholder interests and concerns
  - ✓ Review and gather input on themes and messages
  - ✓ Identify competing ideas and concepts
  - ✓ Confirm standardised themes and messages

13.13 **Adjust.** Planners will need to allow for time to adjust the concept, themes and messages, and communications approach in accordance with insights gained during consultations.

13.14 **Test.** Comprehensive defence will be a new and foreign topic for many of the stakeholders. Once key messages have been developed, it is critical to test all information products and delivery methods with men and women from all sectors of society prior to deploying them in the information campaign.

- No presumptions should be made about how clear the information products are.
- Ask different people within the target audiences how they understand the products presented to them, making sure that no supplementary information is required in order to fully comprehend the messages.
- Ensure the language and images are perceived as neutral, respectful and reassuring.

13.15 **Conduct**. All nations have methods for informing and gaining the support of their populations. These same methods will apply when implementing comprehensive defence and should, therefore, be based on the advice of assigned public affairs and strategic communications experts.

- Some general best practices applicable to comprehensive defence follow:
  - ✓ Do not just talk to the public, involve them
  - ✓ Sponsor contests; e.g., logo and slogan design
  - ✓ Establish public-private partnerships
  - ✓ Encourage and sponsor comprehensive defence-related museum displays
  - ✓ Commission an annual Comprehensive Defence Day[37]
    - Should coincide with a meaningful historical national event
    - Not meant to be a bank holiday or “day off”
    - Military and other public servants engage with the population
    - Theme is population’s role in comprehensive defence
    - Place emphasis on resilience, to include safety, survival, etc.

13.16 **Feedback.** Information is typically transmitted within a community in person through word-of-mouth or via the internet. The spread of incorrect information or

[37] Singapore’s Total Defence Day provides an example https://www.sdc.com.sg/total-defence-day

rumour can be swift and far-reaching. It is essential, therefore, to closely monitor how the information campaign is being interpreted by the target population. This is often done best through the mobilization of trained volunteers and trusted community focal points who can report rumours and uncertainties to the planners as well as address misinformation or confusion they come across within their communities. This does not, however, replace the need for direct interaction with the different communities – listening to concerns, answering questions and reinforcing or adjusting key messages.

13.17 **Sustaining the information flow.** The information campaign discussed in this chapter is focused on gaining broad national concurrence to begin implementing comprehensive defence. However, continuous two-way communications will be required to sustain the public commitment and willingness to sacrifice that comprehensive defence relies upon. All of the principles and many of the methods presented here continue to apply to the enduring information programme, as well as the comprehensive defence education programme.

Table 13.5 Key Take Aways--Concurrence

- **To implement comprehensive defence, the 2% must have broad concurrence from the 98%**
- **Support is gained and maintained through a deliberate, transparent process designed to inform and respect the will of the people**

Intentionally blank

Chapter 14 —Coordination Architecture

This chapter presents best practices for adapting interagency coordination architecture to enable the "98%" to participate in the nation's comprehensive defence collaboration and decision making processes.

Section 1—Overview

14.1 Chapter 4 noted that governments and societies generally lack the organisational structures necessary to allow the 98% to directly support or contribute to national safety and security. This chapter notes that societies also lack the structures necessary to allow the 98% to participate the comprehensive defence assessment, planning or response efforts.

14.2 Throughout the late 20th century and extending into the first two decades of the 21st century, many nations reorganized their governments in an effort to increase cooperation among the agencies responsible for preventing or responding to threatening events. State disaster response, security and defence functions are now commonly performed by a network of interagency teams.

14.3 When implementing comprehensive defence, nations have learned to build upon their interagency architecture in order to incorporate members of the private and civic sectors into the "teams-of-teams" network.

14.4 The nation's goal with respect to establishing comprehensive defence coordination architecture, is to link the public, private and civic sectors at the national, sub-national (or regional) and local levels. The network that results will allow appropriate stakeholders to provide their perspectives and subject matter expertise, and make decisions as required.

14.5 Some entities within the existing governmental structure do not need to be modified at all; some are altered or assigned different responsibilities; and some structures are added.

14.6 The network also includes elements (nodes) that lie completely outside of the government's control. For example, a local fishing club may agree, on a strictly voluntary basis, to perform a function within the nation's coastal watching network. The club will need to be formally integrated into the network so that it can contribute to those aspects of comprehensive defence that relate to its responsibilities, to include participating in assessment and planning processes.

14.7 When implementing comprehensive defence a nation will almost certainly need to establish new laws and policies to support whatever model is adopted (see Chapter 7).

Table 14.1 Key Point—Comprehensive Defence Architecture requirement

Comprehensive defence architecture must facilitate the government's responsibility to guide the processes associated with preparing for, responding to and recovering from threatening events, while also accommodating whole-of-society participation

Section 2—Coordination Architecture

14.8 **Functions.** Comprehensive defence coordination architecture needs to support three functions.

- Decision making
  - ✓ Access to necessary advice, expertise and perspectives
  - ✓ Ability to communicate guidance and decisions
- Coordination
  - ✓ Ability to synchronise the activities of two or more entities to achieve the directed outcome
- Collaboration
  - ✓ Ability for all stakeholders to collectively consider advice, expertise and perspectives when designing solutions or recommendations; i.e., assessments, plans, etc.

Table 14.2 SOF participation within the coordination architecture

So What for SOF
Coordination architecture to include SOF in discussions at all levels when dealing with matters regarding defence against malicious acts • Must maintain highest possible situational awareness • Unique perspective on adversary irregular capabilities and likely courses of action • Responsible for enabling the civic sector resilience and responses o ADC and Home Guard training and employment

14.9 **Components.** The coordination architecture comprises a leadership component and a collaboration component**.**

14.10 **Leadership Component**. The leadership component is responsible for making governmental decisions, issuing guidance and direction, and overseeing action.

- Practical examples include leading assessment and planning efforts, developing situation reports based on information provided by stakeholders, overseeing and coordinating activities within assigned area of responsibility and with parallel entities, coordinating information efforts, etc.
- Three models that can be used by nations organising their leadership component are lead agency, council and tailored. Some nations might establish a blended construct by combining elements from more than one model.

- The approach may vary at different levels. For example, although the objective is to include all stakeholders to the greatest degree possible, the national level will most always maintain a clear hierarchical structure (Figure 14.1 left). The structure may become flatter at the sub-national and local levels, where the network is designed to accommodate more stakeholders (Figure 14.1 right). In either case, all stakeholders must be linked to a single, appropriately appointed executive entity.

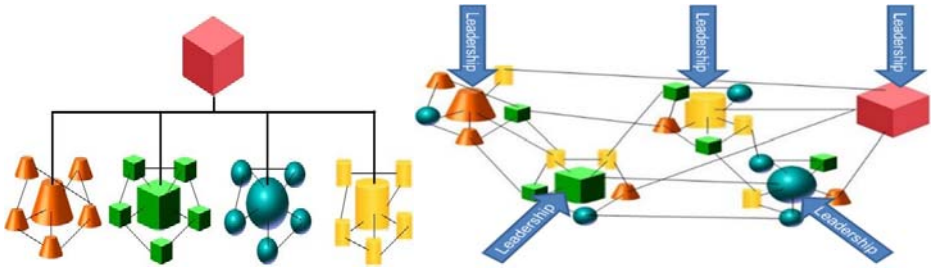


Figure 14.1 Hierarchal vs. networked structure

14.11 Leadership component models

Table 14.3 Considerations for leadership component

Model	Description
Lead agency	• A single agency that currently exists within the government structure may be responsible for coordinating all aspects of comprehensive defence—assessment, planning, establishment, sustainment and execution. • Not be expected to possess expertise in all disciplines. • Must be granted the authority necessary to convene and direct stakeholders. • Most often, the Ministry of Interior (MOI) (or equivalent) is designated as lead agency • Separate lead agencies may be designated for different functions; i.e., assessments, planning, emergency response, defence
Council	• Council is a component of the government • When designated as the principal coordinating body, the council is not subordinated to a lead agency • Normally directly subordinate to an executive decision-making body • Council membership should be a full-time responsibility
Tailored agency	• A third option is to create a new agency for the specific purpose of coordinating Comprehensive Defence • Similar to the lead agency model, with the exception that it is purpose-built

Model	Description
	• The new agency may be formed by combining one or more agencies • An alternative is to transfer components of existing agencies into the new agency • Nations also form new agencies to conduct specific comprehensive defence functions o The most common new functions are cyber security and psychological defence o These functional agencies should not be confused with tailored lead agencies

14.12 **Collaboration Component**.

a. The examples In Table 14.3 are not necessarily unique to comprehensive defence. As noted, most nations employ constructs similar to the ones cited above to facilitate interagency coordination. Few, however, contain provisions for private and civic participation.

b. The collaboration component of the comprehensive defence network must be designed to facilitate the flow of information between government and society.

c. The component normally comprises a collection geographically and functionally aligned councils responsible for facilitating awareness and providing advice to decision-making and coordinating bodies.

d. Councils within the collaboration component contain members from all sectors of society, based on their interests and intended contributions. A council may be permanent or ad hoc and the frequency of meetings will vary depending on its specific function.

Table 14.4 Best practice--collaboration component

Best Practice

- In addition to assigning an overall lead, identify critical social functions and designate an agency to coordinate each
  - o Crisis management (Ministry of Justice)
  - o Defence (MOD)
  - o Health care services (Ministry of Health)
  - o Rescue Services (Ministry of Justice)
  - o ICT security in the civilian sector (Ministry of Justice)
  - o Nature and environment (Ministry of Climate & Environment)
  - o Supply security (Ministry of Trade, Industry and Fisheries)
  - o Water and sewage (Ministry of Health)
  - o Financial services (Ministry of Finance)
  - o Electronic communication services (Ministry of Transport and Communications)
  - o Transport (Ministry of Transport and Communications)
  - o Satellite-based services (Ministry of Transport and Communications)

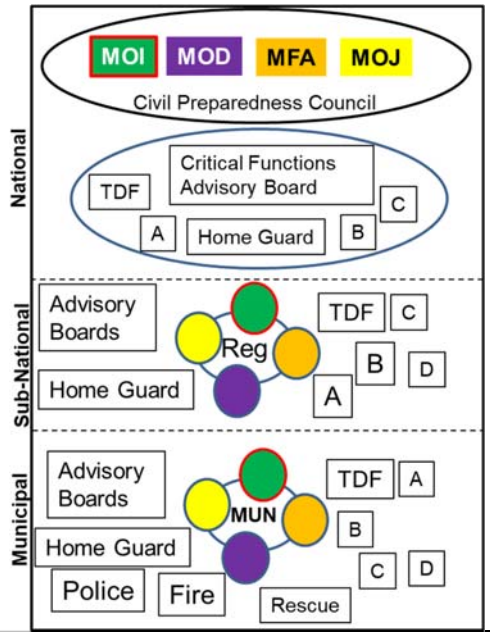
Variation

- Alt Alternatively, the nation may opt to consolidate the critical functions within the pillars and assign an agency to coordinate each pillar
  - o Social and Psychological (Ministry of Health)
  - o Economic and Essential Services (Ministry of Finance)
  - o Military (MOD)
  - o Cyber (Ministry of Justice)
  - o Civil Defence (Ministry of Interior)
  - o Internal and Border Security (Ministry of Justice)

14.13 **Example Comprehensive Defence Architecture**. Table 14.5 contains a notional construct based on related best practices applied by several nations.

Table 14.5 Sample Comprehensive Defence Architecture

National Level.	• The Civil Preparedness Council is created to facilitate interagency coordination among key government stakeholders o MOI (lead agency) o Ministry of Defence (MOD) o Ministry of Foreign Affairs (MFA) o Ministry of Justice (MOJ) • Other ministries and agencies participate as required o Established architecture serves as a “docking station” • The government also established forums to facilitate coordination and collaboration with members of the private and civic sectors o Critical Functions Advisory Board (CFAB)

The nation appoints the Ministry of Interior (MOI) as the lead agency responsible for overseeing civil preparedness matters. 	▪ Notional body comprising private sector actors whose businesses provide critical goods or services (IT, satellite, food, etc.) o Home Guard o Asymmetric Defence Component (ADC) o Others as identified through stakeholder analysis (see Chapter 10)
Sub-national Level	• Similar structures were formed at the sub-national (or regional) levels and linked by to the national bodies • The nation combined several regions to create “clusters” to streamline coordination and collaboration o By clustering the nation reduced 34 geographic regions to 8 o One regional leader is designated to lead each of the 8 clusters
Municipal Level	• The municipal level has more stakeholders, and stakeholder interests are more diverse o At the national level, for example, police, fire and rescue are all represented by a single agency. o At the municipal-level each is independently represented. • Structures were created to allow for coherent private and civic sector collaboration and coordination o For example, individual recreational and commercial fisherman who do not normally belong to any sort of organisation agreed to systematically report any suspicious activity and

	provide emergency evacuation should the need arise o Municipal and sub-national authorities arranged for the formation of a Coastal Watchers Advisory Board to help facilitate the flow of information, advice and expertise between the government and the fishermen. o One member of the board is included in a main advisory board that interfaces with the municipal-level Civil Preparedness Committee

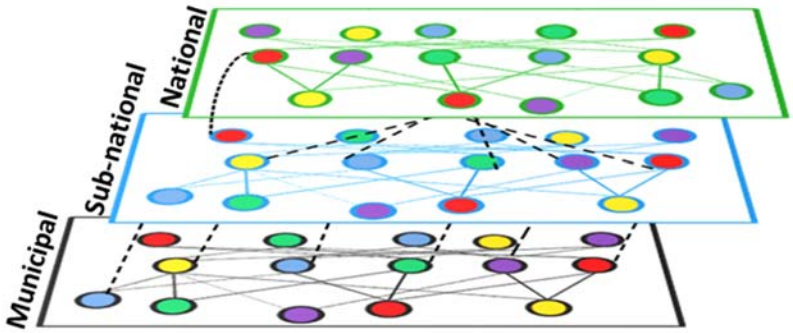


Figure 14.2 Flat architecture

Table 14.6 Key Takeaways--Collaboration Architecture

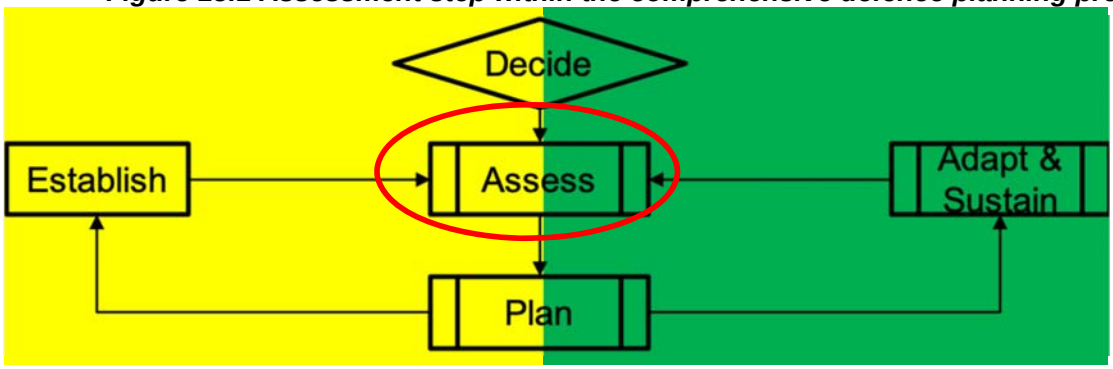
- When expanding the field of stakeholders involved in national safety and security the nation will need to make specific provisions to facilitate meaningful participation.
- A guiding principle is for the resulting structure to be as flat as possible, while ensuring clear roles and responsibilities at all levels—national, sub-national, and regional (Figure 5-2).
- In this sense, the required adjustments are often as much a matter of changing mindsets than making actual structural or procedural changes to existing coordination infrastructure.

Intentionally blank

Chapter 15 –Comprehensive Risk Assessment

This chapter offers a whole-of-society process for assessing potential natural, accidental or malicious threats to the nation's safety and/or security.

Figure 15.1 Assessment step within the comprehensive defence planning process



Section 1—Overview. The decision to adopt Comprehensive Defence initiates a three-step process, which begins with a Comprehensive Risk Assessment (CRA) (Figure 15.1; left side).

15.1 The 3-step process offered in section 15.5 below provides a useful foundation for understanding and designing a CRA that is tailored to a nation's needs. The objective of the CRA is to establish "a common understanding among stakeholders of the risks faced in a country" by identifying and analysing the potential impact of natural, accidental and malicious acts "that require a response at the national or supra-national level."

- After a nation establishes Comprehensive Defence, the process evolves into a cycle (Figure 15.1; right side).
- The cycle recommences with periodic assessment updates.
- The data from the updates is used to revise plans and adapt defences, as may be required.

Section 2—Process. The methodology presented here draws heavily from the United Kingdom's well-established *National Risk Register* and the European Union's *Recommendations for National Risk Assessment for Disaster Risk Management in EU*[38].

15.2 The CRA process offered below builds upon the UK and EU approaches by further accounting for malicious acts as part of the range of threats to national safety and security.

[38]See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61934/national_risk_register.pdf
https://publications.jrc.ec.europa.eu/repository/bitstream/JRC114650/jrc114650_nrarecommendations_updatedfinal_online1.pdf

15.3 **Preparation**. Nations, regions and municipalities must conduct significant prior to conducting CRAs. Below are some factors to take into account prior to commencing a CRA.

Table 15.1 CRA preparation considerations

Factor	Consideration
Structure	• Nations may rely on a single CRA or have separate supporting CRAs at the sub-national and municipal levels
Unity of Effort The CRA requires input from a wide range of stakeholders across all three sectors of the population—private, public and civic. Therefore, it is important to establish unity of effort.	• Grant a single government authority, at each relevant level, the mandate necessary to harmonise the efforts of all participants. • Organize working groups and review boards to ensure appropriate subject matter expert and stakeholder participation throughout the assessment process • Evaluate, and if necessary, revise laws and policies to support information sharing across government and non-government entities • Ensure all appropriate information can be shared with stakeholders o Personnel working within public and private institutions are often conditioned to protect information, either for national security or corporate proprietary reasons o Thus, each participating organisation will likely need to review and refine internal policies and procedures to allow for the required level of collaboration, while still protecting information that would be inappropriate for public release ▪ Provisions need to be made for sensitive law enforcement and intelligence information ▪ Private sector entities involved will need to balance proprietary and security restrictions ▪ The public and civic sectors will be forced to acknowledge that commercial and industrial espionage are legitimate concerns from a business perspective ▪ Publicly releasable versions of the CRA will be required to support coherent whole of society planning and execution
Assessment process expertise	• Establish a pool of personnel professionally trained in assessment procedures o Most participants do not require specific training in the assessment process o However, it is helpful to establish a collection of personnel, distributed across the community of practice, who are responsible for understanding and maintaining the nation's official assessment process o When assessments are conducted or updated, these assessment experts will help guide participants through the officially agreed process
Building the Assessment COP	• Assemble appropriate stakeholders and subject matter experts (see Ch. 12). • Much of the required expertise will reside outside of government.

Factor	Consideration
	• Develop procedures for inviting, encouraging and recognising private and civic sector participation
Assessment COP Sub-structures	• Organise assembled stakeholders into teams, working groups, review panels, etc., as required. • Most stakeholders will participate in more than one team. • Choose the right leaders. o Knowledge o Ability to relate to team members from all sectors of society o Ability to motivate team—many members are participating voluntarily
Assessment Time Horizon	• Determine the assessment horizon o Forecast a minimum of 5 years into the future o A 15 year assessment horizon most useful o If 15 year or longer horizon used, organize into near, mid, and long term; i.e., near term: 0-5 years, midterm: 6-10 years, long term: 11-15 years
Data Management	• Establish data management procedures that enable all participants to easily access and edit information in accordance with their responsibilities, while guarding against security breaches o Consider procedural and technical aspects of information management and security. o Build worksheets to support data collocation and sorting.

15.4 **Potential Government Lead**. The Ministry of Interior (or equivalent agency) is normally the best choice for managing a comprehensive, whole of society assessment process.

Figure 15.2 3-step CRA process

15.5 **3-step Process.** The plethora of qualitative and quantitative analytical functions performed in support of a Comprehensive Risk Assessment notwithstanding, the CRA is constructed through a relatively simple three step process (Fig. 15.2) (see Table 17.7—Comprehensive Risk Assessment Process Checklist):

- Identify. Based on subject matter expert (SME) input, the assessment team will develop a comprehensive picture of potential accidents, natural events and malicious acts that would warrant a national or supra-national response.

- Analyse. Next, the team will review the identified risks to determine the likelihood and impact of each, should it occur.
- Prioritise. Lastly, the group will prioritise the risks based on the combined consideration of likelihood and impact. Risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether further action is required.

15.6 **Assessment Products.** Assessment findings will be used to produce several products. To the greatest extent possible, assessment teams should avoid using technical language in final products, so the information can be easily understood by all stakeholders. Below is a list of typical assessment products

- Classified assessment reports
- Unclassified assessment reports
- Civil response-related reports
- Military-related reports
- Quick reference material
  - ✓ Matrices
  - ✓ Graphic representations
  - ✓ Public information guides and pamphlets

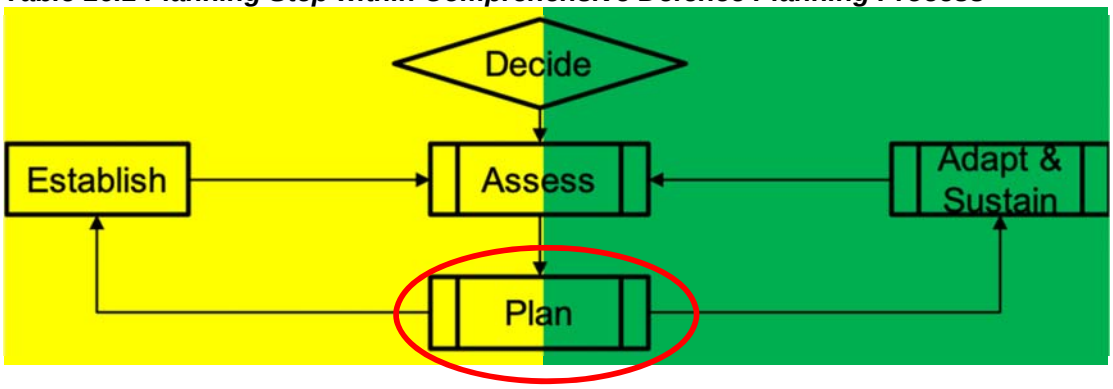
15.7 **Continuity.** Personnel charged with maintaining and updating periodic assessments will change over time. Thus, to ensure continuity, it is important to record, in detail, the procedures used each time an assessment is conducted. This will not impede subsequent assessment groups from modifying the process based on lessons learned and best practices. It will, however, better ensure that the results are consistent from one update to another and save time by eliminating the need to construct new procedures with every assessment.

Table 15.2 Key Take Aways--Comprehensive Risk Assessment

- CRAs are needed to identify the nations vulnerabilities and capability gaps
- CRAs must be continually updated to maintain resilience in a dynamic environment
- The CRA process must be simple and include stakeholders from all sectors of society

Chapter 16 Planning

Table 16.1 Planning Step within Comprehensive Defence Planning Process



Section 1—Overview

16.1 **Introduction.** After completing or updating the Comprehensive Risk Assessment, the next step in implementing or sustaining Comprehensive Defence is to create (or update) a Comprehensive Defence plan.

16.2 Most nations use well-developed planning processes to produce national defence and various disaster prevention and response plans.

16.3 Though they vary in detail by nation, these same processes are adequate and appropriate for creating Comprehensive Defence plans and, therefore, will not be discussed in detail within the handbook. Nevertheless, when planning for Comprehensive Defence, nations must transition their traditional approaches, where civil and military plans are normally addressed separately, to approaches that produce combined civ-mil plans *AND* include civil society as actors within the planning and execution processes.

16.4 Comprehensive Defence plans differ from traditional national plans in three ways:

- Comprehensive Defence planning processes and plans involve the whole of society
- Comprehensive Defence plans combine national defence and emergency response into a single plan or set of plans that address all six comprehensive defence pillars.
- As a subset of the larger planning process, the capability development process must be adapted to account for the whole of society aspect of Comprehensive Defence

16.5 The first two differences are addressed through organisational structures, as described in Chapters 3-5 and Section 2 below.

- To address the third difference, this chapter introduces a Comprehensive Capability Development Process that can be easily integrated into a nation's larger Comprehensive Defence planning process.

Section 2—Comprehensive Defence Planning Considerations

16.6 The following are considerations for developing a two-plan structure to guide considerations comprehensive defence implementation and/or sustainment.

Table 16.2 Comprehensive Defence Plan Structure

Factor	Considerations
Structure	**Part 1—National Security Plan**. • This is the typical charter that nations use to guide their security-focused strategic activities, relationships and investments. • The planning horizon is normally ten to fifteen years, at a minimum. • The difference in the case of comprehensive defence is that the plan will incorporate the private and civic sectors and address natural and accidental threats, as well as malicious acts. • An outline may look as follows: o Summary of Comprehensive Risk Assessment ▪ Natural ▪ Accidental ▪ Malicious o Objectives and goals—At a minimum a national security plan must clearly outline the comprehensive defence goals and objectives; i.e., the 'ends' or desired state to be attained. o Concept for Defence—emphasizing role of private and civic sectors and approaches to the following ▪ Prevention/deterrence ▪ Preparation ▪ Response ▪ Recovery **Part 2—Implementation or Adaptation Plan**. • Procedural component that guides the establishment or sustainment of a comprehensive defence based on the identified objectives and outcome of the most recent CRA • An implementation or adaptation plan identifies exactly how to accomplish the overarching goals by specifying the approaches and resources to be used in reaching those 'ends' – the 'ways' and 'means' • Separating the near-term activities from the long-term strategic approach will help avoid the proverbial trap of "building the plane while in flight" • "Implementation Plan" or "Adaptation Plan" may comprise two components o One component guides resilience ▪ Infrastructure. What physical infrastructure will be created, upgraded or maintained for comprehensive defence purposes?

Factor	Considerations
	▪ Procedures. What procedures need to be implemented or adapted; i.e., strategic communications, information sharing, etc? ▪ Relationships. What relationships need to be established or maintained based on stakeholder analysis? This includes contracts, treaties, etc. ▪ Training and Exercises. What training, exercises and drills need to occur and who needs to participate? o The second component guides active defence measures ▪ Deterrence through strategic communications ▪ Security measures

Section 3—Comprehensive Capability Development Process

16.7 **Preparation**. Procedurally, the planning process is a continuation of the assessment process that precedes it (Ch.15). Of note, many of the stakeholders that contributed to the assessment process will also participate in the planning step, though not all will be needed. So, it is important to conduct a separate round of stakeholder mapping to identify planning team members.

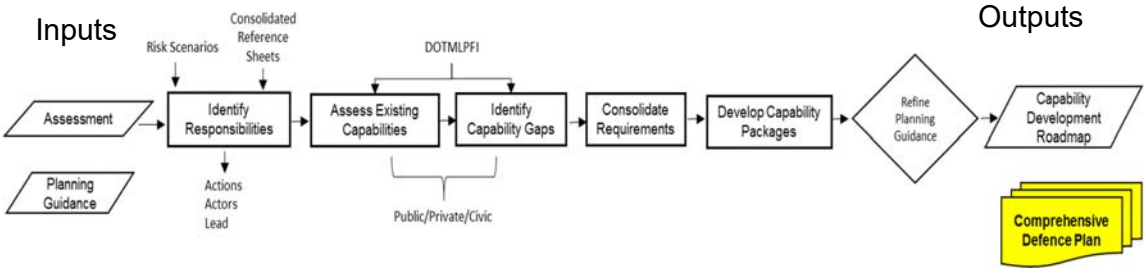


Figure 16.1 Comprehensive Defence Capability Development Process

16.8 **8-Step Comprehensive Defence Capability Development Process.** Per Section 1 of this chapter, the capability requirements and development portion of the nation's defence planning process must be adapted to account for private and civic sector participation in comprehensive defence. Below is an 8-step comprehensive defence capability development process that can be integrated into existing national defence planning procedures.

- Step 1—Issue Planning Guidance
- Step 2—Identify Responsibilities
- Step 3—Assess Existing Capabilities
- Step 4—Identify Capability Gaps
- Step 5—Consolidate Requirements
- Step 6—Develop Capability Packages

- Step 7—Refine Planning Guidance
- Step 8—Develop Roadmap

16.9 **Step 1—Issue Planning Guidance.** At a minimum, planning guidance should address the following three areas:

- Stakeholder sensitivities (Ch. 12 & 13). Comprehensive defence directly involves more stakeholders than is the case with traditional defence. Therefore, it is particularly important for leaders to cite specific interests and sensitivities at the beginning of the planning cycle.
  - ✓ Political
  - ✓ Cultural
  - ✓ Ethnic
  - ✓ Religious
- Legal considerations (Ch. 11). Planners must be aware of the implications of any legal considerations that are unique to any phase of a whole-of-society approach to defence.
- Resource considerations. One of the objectives of the planning process is to identify resource requirements. Where there are more requirements than available resources, planners must determine the risks the shortfall(s) create. Therefore, planners should not be overly constrained by resource limitations. Nevertheless, to ensure realistic plans and risk analysis, planners should be given general guidelines at the beginning of the planning process.

16.10 **Step 2 –Identify Responsibilities**. Use the risk scenarios created during the Assessment Phase (Table 17.7), along with the Consolidated Reference Checklists to accomplish the following:

- Determine what actions need to be taken to prepare for, respond to, and recover from each identified risk
- Determine who performs each action; i.e., associate each action with an actor or set of actors
- Identify a government agency that will coordinate or lead the effort, sometimes called competent authority.
- Example (list not meant to be exhaustive)

Table 16.3 Sample Responsibilities Matrix

Risk: Terrorist attack in a crowded area			
Action	**Actor(s)**	**Lead Agency**	**Remarks**
Activate First Responders	• Fire • Medical • Police • Military • Volunteer orgs	Local Emergency Response	Respond to attack •Fire •Medical •Emergency utilities

Risk: Terrorist attack in a crowded area			
Action	**Actor(s)**	**Lead Agency**	**Remarks**
Heighten National Alert Status	Crisis management centre	MOI	• Place follow-on responders on alert • Prepare for additional attacks
Communicate Event to public	• Media • Crisis management centre	MOI	Inform public of event (5Ws)

16.11 **Step 3—Determine Capability Requirements**. Using the Capability Development Integration model (DOTMLPFI), determine capabilities required for each actor to conduct its comprehensive defence responsibilities identified in the previous step:

Table 16.4 Capability Requirements Matrix

	Public	**Private**	**Civic**
Doctrine	• Authority to act • Plans in place to respond • Training Standards for response	• Terrorist Response Plans checklists • Authorities to act in best interests	• Civic response plans • Training standards (groups/individuals • Reporting mechanisms
Organisation	• Task Organization; C2 Nodes • Communication flow • Liaisons	• Outreach cells • 24/7 response number	• Liaisons • Enablers support
Training	• Terrorist Response training • Individual Skills training	• Civic/Public integration training • Support to first responder training	Terrorist Response training (medical, mental, support)
Materiel	• Response Equipment • Mobility equipment	Medical Supplies	Medical Supplies
Leadership	• Key Leader engagements • Decision support tools	Public Presence	• Key Leader engagements • Public Presence
Personnel	• On-call teams		• Stand-by teams • Immediate first responders
Facilities	• Staging areas • Triage areas	• Triage areas • Protection	• Triage areas • Field hospital areas
Interoperability	• TTPs • Private/Civic response plans	Public/Civic response plans	Public/Private response plans

Step 4—Identify Capability Gaps. Determine what, if any, capability requirements from the previous step must be procured or developed

16.12 **Step 5—Consolidate Capability Requirements.** Compare capability gaps associated with all actions to identify commonality across sectors and phases

16.13 **Step 6—Develop Capability Requirements Packages**

- No standard format.
- Should include cost estimates (personnel, money, time)

16.14 **Step 7—Make Resourcing Decisions and Refine Comprehensive Defence Concept.**

- Based on cost estimates
- Calculate risk for each resourcing decision

16.15 **Step 8—Create Capability Development Roadmap**

- Guide for acquiring and integrating new capabilities
- Reference point for periodic preparedness and capability assessments

Table 16.5 Key Take Aways--Planning

- **The Capability Development Roadmap should not be confused with the Comprehensive Defence Plan**
- **The Roadmap, which principally accounts for resources, or the "Means" within the "Ends/Ways/Means" construct, is a critical component of the plan, but not the plan itself**

Chapter 17 —Comprehensive Defence Planning Tools

This chapter contains checklists and templates to aid with the comprehensive defence assessment and planning processes.

Section 1—Overview

17.1 Comprehensive Risk Assessment Tools

- Section 2 of this chapter comprises checklists, templates and further considerations designed to help guide planners through the comprehensive defence assessment and planning processes.

17.2 Consolidated Reference Checklists

- Section 3 comprises step-by-step checklists designed to guide the overall risk assessment process.
- Describes measures that can be taken within each of the six pillars to achieve the desired level of resilience, and if required, respond to a threatening natural, accidental or malicious event or act
- When used in conjunction with the associated annexes, the CRCs serve as benchmarks for assessing, planning, implementing and sustaining Comprehensive Defence
- When fully realised, CRCs represent an optimally resilient society

Section 2—Comprehensive Risk Assessment Checklist

Table 17.1 Comprehensive Risk Assessment Checklist

Action	Description	References
	Prepare to conduct assessment	
Prep1 - Adjust laws and policies	**Review national, regional and local level laws, policies and procedures to identify potential inhibitors to integrated planning; i.e., information sharing, etc.** • Changes may not be needed immediately, but requirements should be identified as far in advance as possible • Legal and policy adjustments will be necessary throughout the assessment, planning and implementation processes	Chapter 11 (Legal Considerations)
Prep2 - Assemble appropriate stakeholders and subject matter experts	**Account for perspectives of stakeholders from all sectors, along with subject matter expertise from across all domains**	Chapter 12 (Stakeholder mapping)
Prep3 - Identify and train assessment experts	**Establish pool of personnel professionally trained in assessment procedures**	https://www.academiccourses.com/Courses/Risk-Management/Europe/ https://webgate.ec.europa.eu/chafea_pdb/assets/files/pdb/20081103/20081103_d5_00_en_ps.pdf
Prep4 - Organise teams, working groups, review panels, etc., as required	**Assessment group will comprise a team of teams:** • Arrange teams according to stakeholder roles and subject matter expertise. • Many members will be assigned to more than one team. Team leaders must be able to lead diverse, multi-sectoral team	
Prep5 - Determine assessment horizon	**Assess potential risks a minimum of 5 years into the future** • 15 year assessment horizon most useful	

Action	Description	References
	• If 15 year or longer horizon used, may be helpful to organize into near, mid, and long term (i.e., near term: 0-5 years, midterm: 6-10 years, long term: 11-15 years)	
Prep6 - Establish data management procedures	**Assessment team members must be able to access and edit data in accordance with their responsibilities** • Data storage • Access control • Worksheets for collecting and sorting data	Worksheets to support data collocation and sorting (Tables 17.3 thru 17.5)
	Step 1: Identify risks and hazards	
ID1 - Identify planning assumptions	**Assumptions are used to fill information gaps, which if not otherwise filled would prevent further planning** • Should be focused on external factors (environment, potential threats, etc.) • Continually seek to validate and replace with facts when facts become known	Example assumptions • Rains will cause threatening floods twice within the next 5 years • Terrorist organisation will seek to conduct attacks during the 20XX World Games • Adversarial neighbour will employ weaponised information to influence our 20XX elections
ID2 - Based on SME input, develop a comprehensive picture of potential accidents, natural events, and malicious attacks that would warrant a national or supra-national response	**SMEs will employ a wide array of tools during this portion of the process** • Intelligence reports and resources (particularly for identifying malicious threats • Military defence plans • Loss and damage data bases • Maps of relevant research projects • Past risk assessments • Accident investigations **Results will be based on a combination of expert judgement and scientific process**	Table 17.2 Risk Examples

<table>
<tr><th>Action</th><th>Description</th><th>References</th></tr>
<tr><td></td><td>• Qualitative—risk narratives based on expert judgement
• Semi-quantitative—categorise risk according to subjectively assigned comparative scores
• Quantitative—probability estimated using statistical analysis</td><td></td></tr>
<tr><td>ID3 - Develop scenarios to describe each risk</td><td>Scenarios will provide the realistic context necessary for planners to assess likelihood and impact associated with each risk
• Scenarios should include trigger events along with descriptions of possible consequences from cascading events</td><td>National Risk Assessment for Disaster Risk Management in EU (pg 30)
https://ec.europa.eu/jrc/en/publication/recommendations-national-risk-assessment-disaster-risk-management-eu</td></tr>
<tr><td colspan="3">Step 2: Analyse risks and hazards</td></tr>
<tr><td>AN1 - Develop agreed, approved metrics to help communicate probability and impact</td><td>Establish taxonomy for measuring probability and impact of risks, such as the following:
<table>
<tr><th></th><th>Probability</th><th>Impact</th></tr>
<tr><td>1- Very Low</td><td>Improbable</td><td>Negligible</td></tr>
<tr><td>2- Low</td><td>Remote</td><td>Marginal</td></tr>
<tr><td>3- Moderate</td><td>Moderate</td><td>Occasional</td></tr>
<tr><td>4- High</td><td>Probable</td><td>Significant</td></tr>
<tr><td>5- Very High</td><td>Frequent</td><td>Very High</td></tr>
</table></td><td>Tables 17.3 thru 17.5</td></tr>
<tr><td>AN2 - Based on risks scenarios, calculate the likelihood of each event using agreed, approved metrics</td><td>Tools and modelling methods such as those referenced in section ID2 above will continue to prove useful
• During steps AN2 and AN3 identify “Exposed Assets” and analyse “Vulnerabilities” associated with each asset
• For natural events and accidents consider historical, statistical and scientific data, etc.
• Malicious attacks more subjective and likely have a strong classified dimension</td><td>National Risk Assessment for Disaster Risk Management in EU (pg 47, 93)
https://ec.europa.eu/jrc/en/publication/recommendations-national-risk-assessment-disaster-risk-management-eu
UK Risk Register
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attac</td></tr>
</table>

Action	Description	References
		hment_data/file/61934/national_risk_register.pdf
AN3 - Based on risk scenarios, calculate the impact of each event using agreed, approved metrics	**Consider the following**: • Number of fatalities directly attributable to the event • Human illness injury • Impediments to government functions • Infrastructure damage • Economic damage • Social disruption o Access to healthcare o Access to schools o Interruption in supplies o Interruption in essential services (food, water, etc) o Evacuation requirements o Psychological impact on wider population (widespread anxiety, loss of confidence in the government, public outrage)	
AN4 - Develop method for aggregating and presenting results	**Produce a combined factor for each risk based on likelihood and impact**	Table 17.5
	Step 3: Prioritise risks and hazards	
PR1 - Develop an agreed and approved prioritisation metric	**Consider three-tier system (i.e., Tier-1; Tier-2; Tier-3)**	UK Risk Register https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61934/national_risk_register.pdf

Action	Description	References
	Publish results:	
Publish assessment Products	**Must be understandable by all stakeholders** • Use plain language • Maps, matrices, public information guides and pamphlets • Must be accessible • Write for release at the broadest level possible	
Record process	**Assessment must be updated periodically** • Continuity of process will allow stakeholders to easily identify and attribute changes over time	

17.3 **Risk Examples.** Below are risk examples of risks that may be identified during the assessment (see ID 2 and AN 4 on Table XX)

Table 17.2 Examples of Risk

Natural events	✓ **Severe weather** o Typhoon/Hurricane o Heavy snow o Heat wave o Drought o Flooding (Coastal, Inland) ✓ **Earthquakes** ✓ **Volcanic activity** (consider the impact the 2010 Eyjafjallajökull eruptions had on air transportation) ✓ **Human disease** ✓ **Animal disease** o Non-zoonotic ▪ Cannot be transmitted to humans, but affects food supplies, etc. o Zoonotic ▪ Can be transmitted to humans; i.e., rabies, malaria
Major accidents	✓ **Industrial** o Oil or chemical spills o Nuclear power plant o Fires o Technical failure ✓ **Transportation** o Air o Maritime o Road o Rail & underground
Malicious attacks	✓ **Crowded places** ✓ **Critical infrastructure (electricity, water, etc)** ✓ **Transport systems** ✓ **CBRN** ✓ **Electronic** ✓ **Cyber intrusion** ✓ **Weaponised information** ✓ **Armed incursion**

17.4 **Example Worksheets (Prep 6).** The worksheets that can be used as templates when conducting CRA.

- **Example Event Matrix (step AN2)**
  - ✓ Provides a summary of identified risks, alongside the likelihood and potential consequences should the identified event occur
  - ✓ Level and type of detail can vary according to working group preferences

Table 17.3 Example Event Matrix

Category	Event	Likelihood (1-5)	Consequence
Natural	Human Disease[39]	**3**	In the absence of early or effective interventions to deal with a pandemic the following consequences are probable: • significant social and economic disruption • significant threats to the continuity of essential services • lower production levels • shortages and distribution difficulties
	Flooding in the Somewhere Valley	**4**	Some mitigating measures were implemented in response to rain induced floods of 2010; however, as rainy seasons become increasingly severe, the risk of flooding increases • An extremely wet rainy season would put 24,000 homes and 3,200 businesses at risk of flooding • Primary transport routes close • Large numbers require evacuation • Electricity, telecommunications and water supplies interrupted
	Volcanic Activity from Mt. Lamp	**2** Analysis conducted by volcanologists	• Populations of Whoville (120,000) and Whatville (85,000) would require evacuation • 3 of 7 major fisheries inoperable for undetermined period • Main East-West road and rail networks severed

[39] May also be caused by malicious attack

Category	Event	Likelihood (1-5)	Consequence
		from Whoville University	
Accident	Major Transport Accident • Aviation in one of nations 3 major urban areas • Rail • Maritime accident in the Wet Sea • Road	**2**	• Casualties and fatalities • Damage to property and infrastructure within the affected area, potentially leading to a need for evacuation or temporary housing for those affected • Depending on the nature of the incident, contamination and environmental damage
	Industrial	**2**	• Potential disruption to non-essential services causing widespread inconvenience and difficulties for service users • Potential for wider economic impacts.
Malicious Attack	Weaponized Information	**5**	• Undermine social cohesion and national pride • Undermine public trust in government • Influence political decisions • Influence political elections • Cause nation and population to expend resources unnecessarily • Spread fear
	Terrorist Attack on Crowded Public Place	**3**	• Disrupt tourism (economic impact) • Influence political elections • Cause nation and population to expend resources unnecessarily • Widespread fear, panic • Undermine trust in government

Category	Event	Likelihood (1-5)	Consequence
	Terrorist Attack on Critical Infrastructure (transportation, communication, health, industrial)	**2**	• Same physical impact as natural or accidental event • Social, psychological and political considerations beyond those associated with damage caused by natural or accidental event
	Cyber Attack on Infrastructure	**3**	• Critical systems fail (water, electric, communications) • Physical damage resulting from failure • Widespread fear, panic • Misdirected response resulting from misattribution
	Small-scale CBR Terrorist Attack	**3**	• Widespread fear, panic • Substantial expenditure of resources
	Cyber Attack: Data Confidentiality	**3**	

- **Consolidated Risk Prioritisation Matrix**
  - ✓ Summarises risk likelihood and impact, and assigns a tier[40]
  - ✓ Malicious acts highlighted in yellow for ease of reference

Table 17.4 Consolidated Risk Prioritisation matrix

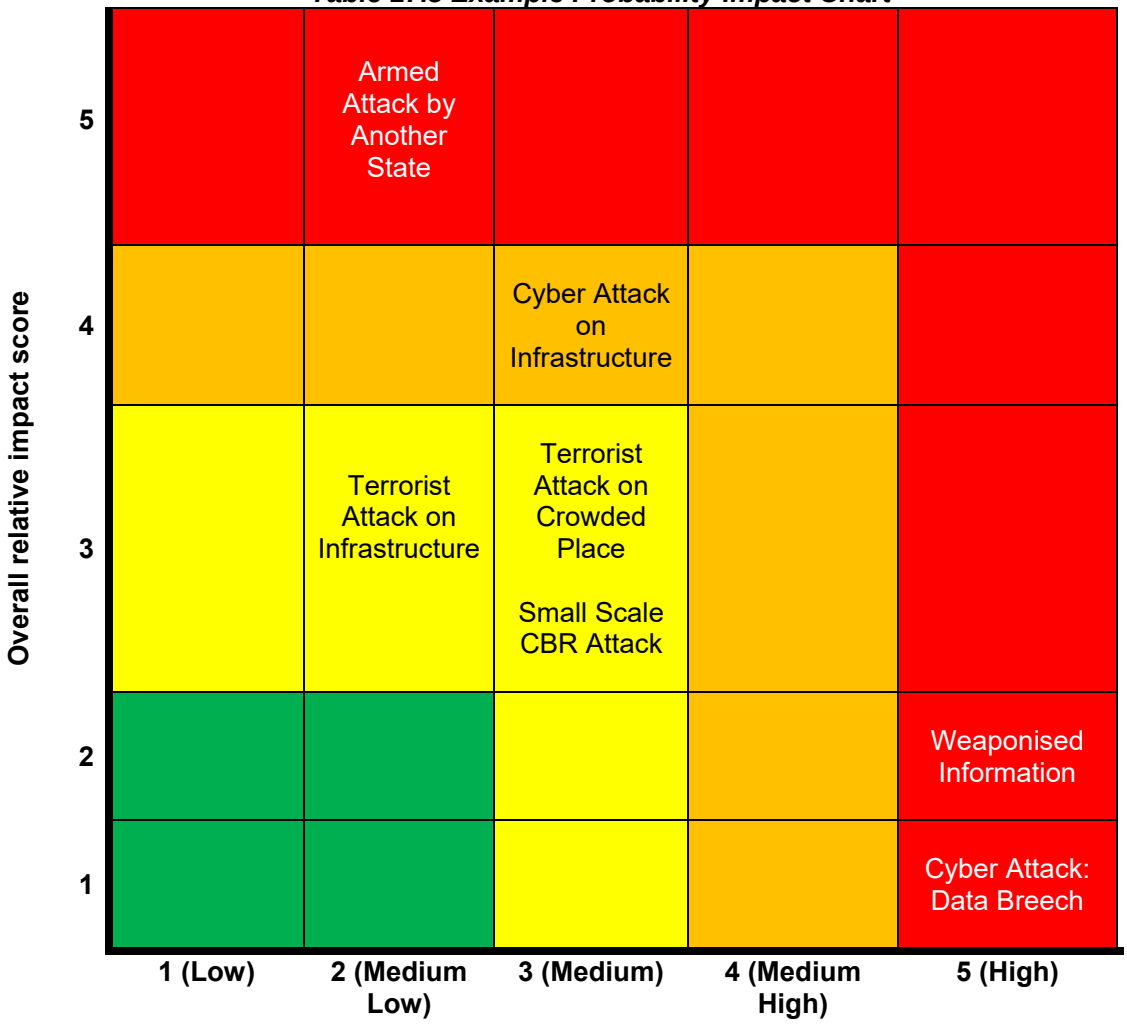
Event	Likelihood (within next 5 yrs)	Impact	Tier
Cyber Attack on Infrastructure	**3** Numerous attempts are made every day; most are not attributable	**4** Depending on severity of the attack	**1**
Human Disease	**3**	**4**	**1**
Terrorist Attack (physical) on Critical Infrastructure (transportation, communication, health, industrial)	**3**	**3**	**1**
Terrorist Attack on Crowded Public Place	**3**	**4**	**1**
Weaponized Information	**5** Continuously occurring	**2** Steadily undermines national self-determination	**1**
Flooding in the Somewhere Valley	**4**	**2** Mitigating measures recently implemented	**1**
Armed Attack by other state	**2**	**5**	**2**
Small-scale CBR Terrorist Attack	**3**	**3**	**3**
Industrial Accident	**2**	**2**	**3**
Major Transport Accident • Aviation in one of nations three major urban areas • Rail • Maritime accident in the Bottomless Sea • Road	**2**	**3**	
Volcanic Activity from Mt. Lamp	**2**	**3**	

[40] There is no specific criteria for establishing tiers. The purpose of tiers to help prioritize efforts.

Event	Likelihood (within next 5 yrs)	Impact	Tier
Cyber Attack: Data Confidentiality	**5**	**1**	**3**

- **Malicious Act Probability-Impact Chart.** Graphic depiction of likelihood and consequence of malicious acts by the working group

Table 17.5 Example Probability Impact Chart



Section 3—Consolidated Comprehensive Defence Checklist

Table 17.6 Consolidated Checklist

Resilience Condition	Considerations and indicators
Economy capable of withstanding shocks	• **Implement sustainable financial planning and budgeting procedures** • **Reinforce confidence and trust in banking system** o Assured guarantees and back-up reserves in case of collapse
Social and Psychological	
Population has shared sense of national pride	• **Promote community groups** • **Highlight sources of common pride** o History o Natural phenomena, resources and geographic features o Art, literature, music o Sports o Economy o Science o Architecture o Responses and recovery from previous crises
Population has shared sense of national purpose	• Create a shared national narrative • Conduct national campaigns aimed at maintaining shared collective will and commitment to defend nation
Population capable of identifying false or misleading information of national importance	• Ensure free, ready access to accurate information of national importance • Establish public education courses that help the public identify false information • Develop campaigns to highlight such information to the public
Population confident government is resilient and prepared to respond to threats	• Make public aware of Comprehensive Defence plans
Population confident in its ability to contribute to national defence	• Establish forums for routine public-private-civic collaboration • Conduct periodic drills and exercises

Energy	
Government and population have continuous access to reliable energy	• **Conduct periodic risk analyses that evaluate, inter-alia:** o Vulnerabilities associated with critical interdependencies o Physical, Personnel, and Cyber Security o Cyber Security (both Information Technology (IT) networks and Operational Technology (OT) o Potential impact of man-made and natural disasters, as well as pandemic events o Potential impact on military forces and capabilities o The potential impact of Foreign Direct Investment (FDI) in critical nodes and systems o Vulnerabilities associated with potential direct and indirect malign interference? o Legal and operational arrangements o An understanding of national and cross-border critical energy supply dependencies, and energy delivery systems to support prioritization of restoration and protection activities o Energy supply restoration plans o Analysis of the implication of critical emerging technologies, in particular critical communication systems and platforms required for energy OT and IT, and potential impacts on resilience due to compromise or lack of access • **Establish a process for developing proportionate risk mitigation strategies that include preventative and reactive measures** o Establish national arrangements for Public-Private-Civic sector platforms (including protocols to exchange information, mitigate vulnerabilities and national priorities) o Identify and prioritise critical end users and their suppliers (including cross border considerations and critical energy users in neighbouring countries) o Tailor and test emergency measures o Identify critical supply chains and single points of failure o Identify critical personnel required to support essential functions, in the event of severe disruption to workforce availability, such as during a pandemic event? o Identify redundant energy systems (generation, transmission and distribution), with mitigation plans o Encourage regional, municipal, and individual citizen development and use of alternative energy sources such as solar and wind energy
Nation and region maintain up to date preparedness plans, design and construction	• **Existing national energy planning include the following, inter alia:** o Capability to restore to a known, trusted baseline configuration

standards, to mitigate disruptions on energy networks from all relevant threats and hazards	o A mechanism to evaluate the robustness, diversity and availability of energy systems/supply networks in relation to the threats and hazards identified through threat assessment programme o Systematic update/implementation of national procedures and regulatory arrangements to assess the existing and emerging threat environment, including cyber, physical, personnel, hybrid, military, foreign direct investment/ownership/control and natural and man-made hazards, including severe disruption to workforce availability o Public-private sector platforms and/or protocols to exchange threat information, mitigate vulnerabilities and national priorities o Procedures and resources to increase surveillance and, if needed, implementation of response plans for the protection of the national energy sector in crisis situations
Critical energy infrastructure protected from all relevant threats including cyber, physical, manmade and natural hazards	▪ **Establish energy security protocols that in include the following:** o A legislative/regulatory/voluntary framework to protect energy infrastructure from malign impacts on energy consumers (civil/industry/defence), which takes account, inter-alia: ▪ Preventative measures, such as ensuring sufficient oil and gas storage, when faced with demand reductions or restrictions ▪ Reactive measures, including emergency power supply arrangements and release of reserve oil and gas supply, to ensure access to reliable essential services in times of crisis ▪ Redundant personnel resources and/or installation of protection protocols at vulnerable energy assets to minimise cascading effects ▪ Operational physical security arrangements and standards, including possible military protection and protection from insider threat ▪ Measures to secure assured access to critical supply chain components, including access to necessary expertise to maintain and operate critical systems during a crisis ▪ Diversification of supply routes, suppliers and energy resources ▪ Preventive measures ensuring sufficient oil and gas storage which could include the deployment of interconnectors and reverse flows, as appropriate ▪ The monitoring, separation and redundancy of critical systems/nodes between Information Technology (IT) networks and Operational Technology (OT) networks, including isolation from internet, corporate and production networks ▪ Effective Cyber security incident response capabilities to detect, react, respond and recover from cyber security incidents affecting critical infrastructure

	▪ Effective technical and organisational countermeasures at vulnerable energy assets in order to minimise cascading effects ▪ A mechanism to communicate threat and all hazard information between government and industry, including public messaging ▪ A process to monitor and assess foreign direct investment, ownership and operational control of critical systems and infrastructure, as well as the means to ensure continued access in times of crisis ▪ A process to monitor, identify and escalate response to incidents of abnormal activity or patterns impacting energy systems, which could be indicators of a hybrid action ▪ Established information sharing protocols to identify similar patterns in other critical sectors ▪ An 'all-hazards' approach covering critical energy infrastructure protection
Communications	
Maintain accountability of available national systems for warning, alerting and informing the populations, national service providers and critical infrastructure operators/owners	▪ **Identify national systems for alerting the government, first responders, and the public, which account for the following:** o Connect both civil and military services and ensure the interoperability of communications networks o Back-ups/redundancies and a priority communication scheme have been identified (digital and/or analogue, including satellite)? o Comprehensive plan for national warning with pre-defined and tailored messages for mass casualty events integrated into the overall warning system o Special messages for CBRN incidents o Swift message transmission from, and between, national and local levels, including private broadcast media o National/regional/local first responder communications platform or network that can be used during the early phases of an event? Is it centrally coordinated o Includes all first responders, including hospitals o Communications systems for both public warning and internal governmental recipients tested regularly o Relevant, structured measures in place, consistent with international best practices, to address cyber risks to health care facilities/systems and certain equipment

Maintain measures to identify and mitigate the potential risks of foreign ownership, control or direct investment in critical communications systems, networks and services, which have potential implications for national security	▪ Ensure authorities account for outsourcing and/or foreign influence, ownership, control or direct investment in national communications networks, including their supply chains supporting essential services, as well as research and development associated with new and emerging technologies? ▪ Establish procedures or a formal mechanism to identify, evaluate and potentially address/mitigate any national security risks resulting from foreign ownership, control, direct investment
Transportation	
Nation maintains flexible, scalable methods for transportation infrastructure protection	▪ Maintain catalogue of critical transportation infrastructure and routes (rail, road, air, and national waterways) to support national priorities during crises, to include back-up capabilities, such as the use of alternative transport modes ▪ Maintain mechanisms to provide ongoing and scalable physical protection and to ensure business continuity in the event of man-made and/or natural hazards, hybrid threats, cyber risks, and epidemics/pandemics ▪ Regularly exercise and test these mechanisms ▪ Maintain arrangements to prioritise and de-conflict (civil-military) transport requirements in times of crisis ▪ Identify military corridors ▪ Establish mechanisms for military planners and civilian transportation providers to coordinate deployment plans
Establish provisions to requisition, use or dispose of national/ foreign owned transport resources.	▪ Implement collaboration between the public, private, and civic sectors at the national, regional, and community levels to develop plans for civil transportation support to the military and exercise those plans routinely. ▪ Maintain provisions to facilitate national access to or the ability to requisition, prioritise and de-conflict transport resources (transport infrastructure, installations, systems, services and assets) for exercises, operations and declared emergencies, to include the following: o Cover foreign owned and operated critical infrastructure and capabilities o Procedures or a formal mechanism to identify, evaluate and address/mitigate any potential national security risks resulting from foreign ownership, control, or direct investment

Maintain up to date list of key stakeholders (infrastructure and transport providers)	▪ Maintain list of key stakeholders that meet a broad range of possible multimodal transportation scenarios/risks? ▪ Assign national authority responsibility for updating the stakeholder list ▪ Regularly update organisation and personnel changes
Maintain protocol for warning and notifying national transportation authorities	▪ Maintain a protocol for national transportation warning and notification ▪ Assign warning and notification responsibility to national authority ▪ Regularly test and exercise the protocol at local and national level, ensuring wide-scale, long duration disruptions
Supply Chain	
National security of supply arrangements in place	• **Establish national security of supply arrangements that accomplish the following:** o Correspond to a comprehensive national threat and vulnerability assessment that takes account of a variety of scenarios, including terrorism, epidemics/pandemics o Rely on pre-determined stockpiles or national production capabilities and/or contracted stocks o Cover civil (e.g. general practitioners, hospitals, nursing/retirement care home personnel) and/or military requirements o Assure security of supply for at least one month o Consider foreign direct investment/ownership/control of the security of supply arrangements o Take into account the potential break down and/or failure (e.g. longer lasting trade disruption and/or export limitations) of the existing supply chains o Account for the need for essential raw materials and/or active pharmaceutical ingredients o Identify and mitigate national dependencies, together with risks and vulnerabilities (e.g. dependence on external production facilities linked to the supply chain of medical supplies, been identified and mitigated) o Include/leverage pharmacies and/or other relevant retail stores o Include emergency funds/resources available to compensate for- or to purchase relevant resources? o Assure a clear management and administrative structure established for any national security of supply arrangement, managed centrally or through a government agency and/or private sector o Ensure relevant transport assets are available for timely distribution and resupply o Include arrangements to release relevant resources from the security of supply arrangement and/or enable national authorities to steer/direct the production of supplies and/or distribution of assets/resources

	o Evaluate cyber risks to supporting information technology systems and the supply chain, including establishment of a structured process in place, consistent with globally accepted good practice/standards, to address and manage such risks o Include reporting requirements to notify shortages/shortfalls, which are centrally managed and updated regularly o Put in place crisis communications to address questions related to security of supply and access arrangements and potential disinformation/misinformation? o Establish regional and community caches of critical supplies to include non-perishable foodstuffs in order to mitigate supply chain disruption. o Include guidance to citizens on personal resilience
Food and Water	
Nation maintains, as a component of the national risk assessment, an overview of the key food and water infrastructure and resource	• **Establish mechanism to maintain up to date risk assessments that account for the following**: o Essential stakeholders and infrastructure for the production, processing and distribution of food and water resources relevant to resilience and civil preparedness o Methodology/process for identifying threats and vulnerabilities and their severity/probability in each sector o Coordination with relevant intelligence services (for example on likely bio-toxins) o Potential interdependencies on external suppliers; e.g. energy (electricity and fuels), water, transport, (road, air and sea), telecommunications, packaging; feed; livestock; fertilisers; pesticides, and IT systems o Critical elements of the system, procedures and mechanisms for detection, monitoring and response o Foreign direct investment in, ownership/control of critical nodes and systems and possible vulnerabilities associated with such ownership o Potential military requirements and requirements linked to the possible influx of refugees and other large-scale population movement o Critical factors to support essential food and water supply functions, including workforce availability, freedom of movement of goods and labour, in the event of severe disruption, such as during a pandemic event, cyber or hybrid attack and natural disasters
Nation maintains comprehensive overview of resources and key stakeholders relevant to the	• **Establish mechanism to maintain comprehensive overview of the following:** o Relevant resources o Critical operators and stakeholders (public and private) o Approved food establishments and water suppliers

monitoring, detection, testing and reporting of contamination of food and water resources	o Relevant assets and expertise from government as well as from commercial, academic, scientific actors and agencies active in the food and water sector o Key resources from other sectors (e.g. transport) o Customs, sanitary, phytosanitary and veterinary border inspection capabilities. o Specific military capabilities
Comprehensive defence plan includes ways to mitigate identified risks within the food and water sectors	• **Establish sector specific plans to address the following:** o Commercial sector, including business continuity plans or emergency plans o Food and water safety and supply chains, including dependence on production inputs/imports such as fuels; fertilisers; pesticides; packaging materials; maintenance / spare parts; treatment and disinfection products for potable drinking water o Interdependencies such as energy; communications; transport and dependence on Information Technologies o Process to monitor and assess the evolving landscape of foreign direct investment, ownership and operational control of critical systems and infrastructure, as well as the means to secure continued access in times of crisis o Points of Contact at all relevant levels with appropriate decision making authority, including a clear definition of roles and responsibilities and allocation of relevant resources o Potential requirements linked to Host Nation Support, including support to the national military; potential support to reinforcing forces of Allies and support to deal with a possible influx of refugees and other large scale population movements o Potential consequence of future dependencies on new and evolving technologies, such as 5G, for food/water production, systems and services o Critical segments of the workforce and their availability to meet particular vulnerabilities in the event of a long-term disruption caused, for instance, by Chemical, Biological, Radiological and Nuclear (CBRN) events, including epidemics/pandemics, cyber, and natural disasters o Additional safety measures and resources (protective measures, testing protocols, surveillance, physical protection, and personal protective equipment) by government and commercial stakeholders o Information exchange requirements and information means, including for classified information o Coordinated communication, risk and crisis communication to the public, including guidance to the different stakeholders o Appropriate awareness raising programmes

	o Contingency arrangements to ensure the availability of essential elements of the workforce in the entire food and water supply chain, as well as security of supply arrangements? o Potential shifts in demand and consumer behaviour due to crises, as well as appropriate information to the public
Nation maintains an inclusive food and water-specific crisis management and response capability	• **Establish a sector-specific crisis management system and response capability, which includes to following:** o Security of supply arrangements for food and water in crises, including alternate/back-up arrangements o Relevant stakeholders (public, private and civil society as appropriate) o Key actors/suppliers/trade associations responsible for (65, 75 or 80%) of the activity of each sector (i.e. agriculture, food and water processing, logistics, wholesale and retail) o Roles, location and contact details for key personnel/functions with decision making authority and foresee staff rotation for longer term crises o Organisational and personnel changes o Pre-identified relevant points of contact for coordination and supplies to the military o Levels of security clearance for key personnel/functions, including personnel in the private and civic sectors o Relevant monitoring, early warning and reporting requirements (taking into account relevant legislation) o Regular contacts, exchange of information, and consultations between key stakeholders o A system for reporting and information sharing o Bilateral and multilateral cooperation arrangements/information exchange o Essential elements of the workforce, including technical service personnel who have access to essential spare parts, treatment and disinfection products for potable drinking water o Qualified personnel to ensure crisis communication to the public and other stakeholders
Mass Casualties	
Maintain critical assets to deal with mass casualties:	• Coordinate public (military and civil), private, and civic sector assets with emphasis on medical and rescue capabilities as well as transportation. • Include identification of critical healthcare workers (including mental health care providers) required to support essential functions, in the event of severe disruption to workforce availability, such as during an epidemic/pandemic event

	• Include a standard triage algorithm, including pre-hospital and facility-based triage during extraordinary/surge situations • Standard triage system used and first responders trained accordingly • Medical evacuation assets (sea, rail, rotary/fixed wing and ground) available • Relevant CBRN (civil and military) capabilities been included • Hospitals prepared for the management of mass casualties • Emergency plans in place for hospitals • Relevant specialist capabilities foreseen (e.g.: psychological capabilities, turnkeys) • Mechanism to track, trace, and regulate casualties and bed capacities (burns, CBRN, etc) • Includes key pharmaceutical companies; key vaccine stocks/supplies; blood and blood products (including transport); • Mortuary affairs; crematoria and mortuary facilities to handle large numbers; relevant transfer and transport assets; volunteer services that may provide important assets and resources, as well as capabilities for the identification of victims • Information regularly updated • Civil and military, as well as international capabilities, reflected • Security measures in place to ensure first responders are able to respond in a safe environment and have access to personal protective equipment and decontamination capabilities • All authorities have the necessary, independent and integrated portable and mobile communication equipment • Capabilities needed to deal with waste management included
Military	
Population trusts and supports the military	• Educate and inform public on military's roles and responsibilities • Develop programmes to encourage civilians to contribute to military-led efforts • Ensure military reflects cultural and ethnic composition of the nation • Ensure military remains apolitical and professional
Military prepared to integrate civic sector into defence structures in event of an emergency	• Laws in place to facilitate incorporation of public into defence activities • Civic responsibilities planned and rehearsed • Structures formed prior to crisis (i.e., home guard, auxiliary support, etc.) • Periodic training exercises include private and civic sector roles
Cyber	

Nation has a whole of society cyber defence concept[41]	• **Account for all threats, to include, inter alia, the following:** o Cyber criminals o State and state-sponsored actors o Terrorists o Hacktivists o "Script Kiddies" • **Identify roles for all members of society** o Public sector o Private sector o Civic sector • **Develop an easily understandable strategic approach, per the following example:** o Defend ▪ Active cyber defence ▪ Build a more secure internet ▪ Protecting government ▪ Protecting critical national infrastructure and other priority sectors ▪ Changing public and business behaviours ▪ Managing incidents and understanding the threats o Deter ▪ Cyber role in deterrence ▪ Reducing cyber crime ▪ Countering hostile foreign actors ▪ Preventing terrorism ▪ Enhancing sovereign capabilities o Develop ▪ Strengthening cyber security skills ▪ Stimulating growth in cyber security sector ▪ Promoting cyber security science and technology

41 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/national_cyber_security_strategy.pdf

	▪ Effective horizon scanning • **Develop metrics for measuring strategic effectiveness**
National digital systems protected against malicious cyber attacks	• Educate leaders and technicians to recognise malicious cyber incidents • Conduct realistic cyber defence exercises • Develop public-private partnerships with information technology firms • Sponsor public cyber defence competitions • Continually update government-sponsored cyber defence awareness programmes • Enter international cyber defence competitions and exercises • Create mechanisms for detecting, recognising and classifying cyber attacks, including information and intelligence sharing and TTP standardisation • Develop provisions to facilitate government/law enforcement - industry collaboration to recover data in support of comprehensive defence • Create redundant systems and sites
Nation able to continue to function in degraded information systems environment	• **Develop system for classifying cyber attacks impacts; i.e., level of degradation** • **Train & educate to operate when info systems offline** o Paper forms o Manual navigation aids (compass, sextant, etc.) • **Create continuity of operations plan for functioning in degraded environment**
Private and civic sector empowered to contribute to cyber defence	• Establish formal and informal public education programmes at all levels • Encourage industry and academia to report compromises of information, including protective systems • Empower ISPs to take responsibility for preventing and responding to malicious cyber incidents
Internal and Border Security	
National laws, policies, agreements and practices facilitate interagency cooperation in support of internal and border security	• Establish legal and policy frameworks for intelligence and information sharing among ministries and security agencies • Establish legal and policy frameworks to enable military support to internal border and security organisations in event of crisis • Establish multi-ministry, multi-domain border security awareness centre capable of tracking and responding to, inter alia, air, land and maritime access to the nation

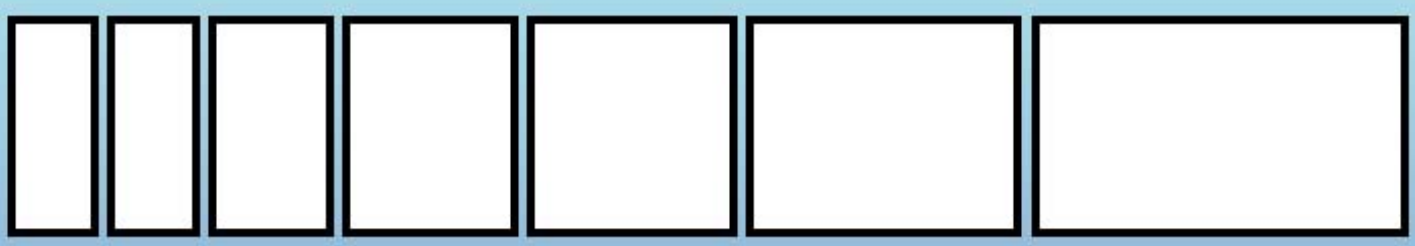
Government enables private and civic sector involvement in internal and border security	• Establish inter-regional coordination capability o Consider regional security clusters ▪ Regional administrative boards ▪ Regional law enforcement agencies ▪ Military bases and units within the region ▪ Healthcare agencies ▪ Municipal public services ▪ Faith organisations: i.e., churches, synagogues, mosques ▪ Volunteer defence organisations • Establish activity reporting programmes • Support and govern the establishment of security oriented civic groups o Neighbourhood crime watch groups o Domain watch (i.e., air, coastal, mountain, satellite) • Develop national pamphlet to describe and promote, inter alia, civic role in internal and border security
Nation able to maintain internal and border security in time of crisis	• **Establish approaches for conducting security functions in case of threatening natural, accidental or malicious event** o Volunteer services o Community group responsibilities • **Incorporate law enforcement and security services into national defence training exercises, alongside the military and civic sector participants** • **Establish approach for interacting with law enforcement organisations in the event of foreign occupation** o Collaboration o Accommodation o Resistance

Movement of Displaced Personnel	
Nation has provisions for potential restrictions on the movement of people under exceptional circumstances, such as an obvious danger of loss of life due to natural disasters; life threatening epidemics, pandemics, Chemical, Biological, Radiological and Nuclear (CBRN) threats; or to support national military requirements (e.g. to prevent interference with the movement of military forces)	• **Establish provisions that take the following into account:** o Applicable international law and regulations dealing with the movement of people and restrictions o Clear communication to the population about the purpose and length of these movement restrictions if predictable; targeted group/groups of people and a clearly established process for recovery o Exceptions for specific groups, such as identified critical personnel (e.g. health care workers and workers supporting other essential services, including child-care, care for aged and disabled people, critical personnel for public utility services, etc.) o Arrangements to allow citizens from other nations to return back to their home countries if they so wish o The social and economic consequences of long-term movement restriction or lockdown, including its impact on the provision of critical public services, in relation to public health priorities
Nation has the ability to deal with uncontrolled movement of people	• **Establish national arrangements and contingency plans to manage rapid mass movement of people and uncontrolled movement of people, to include an influx of persons that exceed the nation's absorption capacity; plans should account, inter alia, for the following:** o Realistic planning assumptions based on risk assessments and the most demanding potential scenarios ▪ Legislation that allows designated organisations to implement population movement plans and operations ▪ Provisions for basic human needs such as physical security, including protection for the most vulnerable groups, sheltering, food, water, health, sanitation and hygiene, psychosocial care, education and transport. ▪ Local faith, service, and other volunteer civic organizations develop plans for community support to displaced persons arriving or transiting through their municipalities until such a time as regional, national, or international aid might become available.

	▪ Measures and arrangements for public health and emergency services (e.g. to create surge capacity, including through civil-military and bilateral/multilateral cross border cooperation, as well as with private/commercial, International Organisations (IOs), and Non-governmental Organisations (NGOs) resources ▪ Provisions for vulnerable persons (e.g. women, children, elderly and disabled people) including but not limited to identification, transport and special needs ▪ Specific public health requirements (e.g. prevention of infectious and chronic diseases, mental health, public health awareness, test facilities and vaccination programmes based on targeted screening or medical intelligence (both incoming and local), health surveillance system, including contact tracing in epidemics); security of supply arrangements for vaccines; drugs, medical supplies and personal protective equipment (PPE); documentation and tracking ▪ Organisational considerations, including a description of the national crisis or emergency structure; relevant juridical framework; roles, responsibilities, and tasks of lead and supporting organisations (e.g., International Organisations, NGO's, and other nations.) ▪ Designated routes/corridors for transporting people and emergency services that do not interfere with the movement of military forces ▪ Capacity requirements, taking into account potential competition amongst surge capacities to support military operations ▪ Comprehensive crisis communication and information considerations to ensure exchange of information, including on transmissible diseases, between key stakeholders, including relevant international organisations. ▪ Procedures for requesting and receiving international assistance ▪ Registration, security screening and tracking of people on the move, including the storage and sharing of information, as appropriate, taking into account as appropriate, with appropriate relevant protection measures and in accordance with national and international law

Intentionally blank

Comprehensive Defence Handbook (A)(1)
Volume I



Published by the
NATO Special Operation Headquarters (NSHQ)