

NO MAN'S LAND: TECH CONSIDERATIONS FOR CANADA'S FUTURE ARMY



National
Défence

Défense
nationale

Canada

Canadian Army Land
Warfare Centre



NO MAN'S LAND: TECH CONSIDERATIONS FOR CANADA'S FUTURE ARMY



Canadian Army Land Warfare Centre

NO MAN'S LAND: TECH CONSIDERATIONS FOR CANADA'S FUTURE ARMY

Canadian Army Land Warfare Centre
Kingston, Ontario
2014

Publication Data

1. No Man's Land: Tech Considerations for Canada's Future Army

Print—English
D2-326/2014E
978-1-100-22961-4

PDF—English
D2-326/2014E-PDF
978-1-100-22962-1

Print—French
D2-326/2014F
978-0-660-21513-6

PDF—French
D2-326/2014F-PDF
978-0-660-21514-3

Cover Design & Text Layout
Army Publishing Office, Kingston, Ontario



This official publication is published on the authority of the Commander, Canadian Army.
No part may be reproduced or republished elsewhere without the express permission of the
Canadian Army Land Warfare Centre through the Department of National Defence.

© 2014 Department of National Defence



FOREWORD

In the future, the world will continue to be fraught with risks that directly challenge Canadian values, national interests and security. The Canadian Armed Forces and the Army are needed to defend Canada, Canadians and Canadian interests in this future security environment. To remain an effective instrument of national power, the Canadian Army must continue to innovate and adapt.

Land Operations 2021, Adaptive Dispersed Operations: The Force Employment Concept for Canada's Army of Tomorrow provides the overarching framework for how the Army will successfully operate in the future operating environment. One of the enabling concepts put forth in this future force employment concept is distributed autonomous systems. Arguably representing a true watershed in human technological achievement, autonomous systems have the potential to revolutionize land operations. Distributed across the battlespace, they will undoubtedly contribute to the Army's ability to conduct adaptive dispersed operations.

Subsequent research by the Army's Future Concepts Team at the Canadian Army Land Warfare Centre (CALWC) has produced some preliminary concepts relating to space and cyber operations. As the world continues to experience unparalleled levels of technological convergence, our ability to exploit these highly technical environments in order to influence land operation will increase dramatically. The relevant chapters in this publication present concepts that together make up a first look at how the Army might best exploit the space and cyber environments while minimizing the associated risk.

This publication forms the basis for further concepts and designs work. It is intended to foster critical and innovative thinking about how the Canadian Army will need to endure to meet the challenges of the future.

R.N.H. DICKSON, CD

Colonel

Director, CALWC

TABLE OF CONTENTS

- FOREWORD..... v**

- CHAPTER 1 · INTRODUCTION..... 1-1**

- CHAPTER 2 · ROBOTS IN THE ARMY:
A STUDY OF UNMANNED SYSTEMS 2-1**

- Part One · Introduction 2-2**
 - 1.1 Aim..... 2-2
 - 1.2 Historical Perspective 2-3
 - 1.3 Mission Analysis 2-4
 - 1.4 Adaptive Dispersed Operations..... 2-8
 - 1.5 The Robot Requirement..... 2-11

- Part Two · Current Capabilities 2-13**
 - 2.1 Canada 2-13
 - 2.2 United States..... 2-17
 - 2.3 Other Developments of Interest..... 2-20

- Part Three · Technological Readiness 2-21**
 - 3.1 Technological Limiters..... 2-23

- Part Four · Institutional Challenges..... 2-29**
 - 4.1 Socialization of the Army to Robot Systems..... 2-29
 - 4.2 Fear..... 2-31
 - 4.3 Leadership Responsibility 2-32
 - 4.4 Build on Experience..... 2-33
 - 4.5 Ensure User-Friendliness 2-34
 - 4.6 Demonstrations 2-35
 - 4.7 Note on Disruptive Technology..... 2-35
 - 4.8 Note on Procurement 2-36

- Part Five · Legal and Ethical Challenges 2-37**
 - 5.1 International Law 2-37
 - 5.2 Responsibility 2-38
 - 5.3 *Jus ad Bellum*..... 2-40

5.4	<i>Jus in Bello</i>	2-42
5.5	Ethics	2-43
5.6	Liability	2-45
Part Six · Impact on the Operational Functions		2-45
6.1	Command	2-45
6.2	Sense	2-47
6.3	Act	2-51
6.4	Shield	2-54
6.4.1	Shield the Robot	2-54
6.4.2	Shield the Force	2-55
6.5	Sustain	2-56
6.5.1	Tactical Logistics Support	2-57
6.5.2	Operational and Domestic Support	2-57
6.6	Task Analysis	2-58
Part Seven · Defining the Capability Requirements		2-59
7.1	Personnel, Leadership, and Individual Training	2-59
7.1.1	Personnel	2-60
7.1.2	Leadership	2-63
7.1.3	Individual Training	2-65
7.1.4	Education and Professional Development	2-66
7.2	Research and Development and Operational Research (plus Experimentation)	2-67
7.2.1	R&D Partnerships	2-68
7.2.2	Technological Research and Development (R&D)	2-69
7.2.3	OR/Experimentation	2-71
7.2.4	Simulation	2-72
7.3	Infrastructure, Environment, and Organization	2-73
7.3.1	Infrastructure	2-73
7.3.2	Organization	2-74
7.4	Concepts, Doctrine, and Collective Training	2-75
7.4.1	Mothership Concept	2-76
7.4.2	Swarming Concept	2-77
7.4.3	Dog Concept	2-79
7.4.4	Other Potential Concepts	2-80
7.4.5	Collective Training	2-82
7.5	Information Management and Information Technology	2-82
7.5.1	The Communications Problem	2-83

- 7.5.2 Interoperability 2-85
- 7.5.3 Latency 2-86
- 7.5.4 Software 2-87
- 7.5.5 Encryption 2-87
- 7.6 Equipment and Support..... 2-87
- 7.6.1 Human Robot Interface (HRI) and Control Units 2-88
- 7.6.2 Ruggedization 2-88
- 7.6.3 Power Considerations..... 2-89
- 7.6.4 Sparing..... 2-89
- 7.6.5 Maintenance and Lifecycle Management (LCM) 2-89

Part Eight · Framework for Robot Systems 2-90

- 8.1 Framework Building Blocks..... 2-91
- 8.2 Classification Based on Autonomy..... 2-93
- 8.3 Individuals and Swarms 2-96
- 8.4 Framework 2-97

Part Nine · Implementation Plan 2-99

Part Ten · Conclusion 2-105

**CHAPTER 3 · ARMY ROBOTICS CONCEPT:
FROM TOOLS TO TEAM MEMBERS..... 3-1**

Part One · Introduction 3-2

Part Two · From Tools to Team Members 3-2

Part Three · The Soldier’s Burden 3-4

Part Four · Robots and the Operational Functions 3-6

Part Five · Integrating the Robot Team Member 3-9

Part Six · Modularity: An Essential Consideration..... 3-11

Part Seven · Other Design Principles..... 3-11

Part Eight · Graphical Model of the Human–Robot Team 3-12

Part Nine · Unmanned Systems Taxonomy	3-14
Part Ten · Conclusion	3-15
CHAPTER 4 · FUTURE CONCEPT FOR ARMY USE OF SPACE-DERIVED CAPABILITIES	4-1
Part One · Introduction	4-2
Part Two · Space Operations Background	4-3
2.1 Space Support	4-4
2.2 Space Control	4-4
2.3 Space Force Application	4-6
2.4 Space Force Enhancement	4-6
2.4.1 Satellite Communications (SATCOM)	4-6
2.4.2 Positioning, Navigation, and Timing (PNT)	4-7
2.4.3 Satellite-Derived Intelligence, Surveillance, and Reconnaissance (ISR)	4-8
2.4.4 Environmental Sensing	4-9
2.4.5 Missile Warning	4-10
Part Three · Capability Deficiency: Assured Access to Space Force Enhancement	4-11
3.1 Potential Options	4-11
3.1.1 Partnerships	4-13
3.1.2 Integral Launch	4-13
3.1.3 Multi-Domain	4-15
3.2 Vulnerabilities	4-15
Part Four · Multi-Domain Concept	4-17
Part Five · Novel Uses of Space	4-21
5.1 Impossible Applications	4-21
5.2 Space-Based Routing	4-22
5.3 Detecting Terrestrial Broadcast	4-22
Part Six · Conclusion	4-23

CHAPTER 5 · FUTURE ARMY CYBER CONCEPT.....5-1

Part One · What Is the Cyber Environment?..... 5-2

- 1.1 The Land, Air, and Maritime Environments 5-2
- 1.2 Why Space *Is* and Why Human *Is Not* 5-3
- 1.3 The Electromagnetic Operating Environment: How Cyber Fits 5-6
- 1.4 Components of the EM Environment..... 5-7
- 1.5 The Case for New Environments: Quantum..... 5-10
- 1.6 A Nano Environment? 5-11
- 1.7 Conclusion 5-12

Part Two · Is Cyber Deterrence Possible? 5-13

- 2.1 Offensive Cyber Capability to Deter Cyber Weapons Development and Proliferation. 5-13
- 2.2 Fighting Fire with Fire: Offensive Cyber Capability to Deter Hostile Cyber Attack..... 5-15
- 2.3 Mutually Assured Cyber Destruction: A Losing Strategy 5-15
- 2.4 Deterrence Through Reducing Cyber Dependence 5-17
- 2.5 Forget Clausewitz: Defence as Deterrent 5-17
- 2.6 Cyber Deterrence Today: A Pipe Dream..... 5-18
- 2.7 An Interim Solution: Welcoming Attack! 5-19
- 2.8 Destroy Anonymity: Welcome Deterrence! 5-21

Part Three · Offensive Cyber Operations 5-21

- 3.1 Offensive Operations Doctrine..... 5-22
- 3.2 Potential Targets for Cyber Weapons 5-22
- 3.3 Cyber Intelligence 5-25
- 3.4 Conclusion 5-26

Part Four · Army Cyber Concept..... 5-26

- 4.1 CNO and EW: No Longer Distinct 5-27
- 4.2 Cyber Operations = Computer Network Operations + Electronic Warfare..... 5-28
- 4.3 The Context of Convergence: C4ISR and Threat..... 5-29
- 4.4 Computer Network Defence and the Cyber Picture..... 5-32
- 4.5 Cyber and the Operational Functions 5-36
- 4.6 Risk Areas 5-38

Part Five · Conclusion and Questions..... 5-39

Annex A · Preliminary PRICIE+G Analysis	5A-1
Personnel and Leadership	5A-1
Research and Development and Operational Research (Plus Experimentation)	5A-2
Infrastructure, Environment, and Organization	5A-4
Concepts and Doctrine.....	5A-6
Information Management and Technology.....	5A-7
Equipment and Support.....	5A-7
Generate	5A-8
Annex B · CYBER and C4ISR.....	5B-1
CHAPTER 6 · CONCLUSION	6-1
BIBLIOGRAPHY.....	B-1

CHAPTER 1

INTRODUCTION

“No man’s land” is a term traditionally used to describe the unoccupied area of ground between opposing military forces, a tract of land epitomizing danger, stalemate or violent dispute. Examples include the dangerous ground separating Allied and German trench lines in the First World War or the Demilitarized Zone between forces of the North and South on the Korean Peninsula today. No man’s land is a place where humans may not easily pass, and the term is therefore appropriate for complex operating environments such as space and cyber. No man’s land may also describe a hostile environ where humans dare not tread—where future machines could lead the way for us.

This book examines three key capability areas that are expected to play a significant role in future land operations. *No Man’s Land* will provide an initial analysis of the future employment of unmanned systems, space-based and cyber-based capabilities. Although the human dimension will continue to comprise the heart and soul of the Army, technology—the tools of warfare—will nevertheless continue to be a critical factor in the success of military operations. Technology on its own is not a capability; it is its interaction with people (through doctrine and training) that transforms it into something capable of dominating the adversary.

The pace of technological change that we have witnessed over the past several decades continues to accelerate, indicating that the technological edge will continue to represent an important advantage. One area that holds the potential to transform future warfare is robotics. The manner in which UAVs have evolved to their current prominence on operations certainly points to increased roles for them as time goes on. They also signal the potential rise in ground-based robotics in future conflict. The utility of employing machines to complete tasks that were once the exclusive domain of the human soldier has applications beyond the air environment. Robots are already in heavy use today supporting explosive ordnance disposal (EOD) and counter-improvised explosive device missions. In the future, as technological limiters are overcome and institutional barriers are breached, robots will play a larger role in areas such as intelligence, surveillance review (ISR), logistics, and engineering support. A cursory look at current global research and development (R&D) efforts in ground-based unmanned systems shows that just about every Army task is being actively examined for “roboticization” of some sort.

This book includes a detailed study of unmanned systems in Chapter 2 followed by a shorter chapter on the Army's current robot concept: from tools to team members. These chapters take a look at potential capability gaps in terms of the future land operating concept (i.e., adaptive dispersed operations) and suggest ways in which robots may be able to fill those roles. Key to understanding where robots may be most appropriately employed in the Army will be determining where they are best able to limit both human cognitive and physical burdens. Robots will be needed that work best in teams, operating beside humans rather than without them. Having a human in the loop should not be confused with robot autonomy. There are all kinds of decisions that humans are not permitted to make and for which they must seek command guidance. The paradigm is the same for autonomous robotics. This book will discuss a framework for robot autonomy and offer discussion of the legal and ethical aspects associated with the use of robots. The reader will also find a preliminary PRICIE analysis of robot capability. "PRICIE is an acronym which describes the Canadian Forces functional components of capability. A complete analysis will examine all aspects of a capability including: personnel, leadership and individual training; research and development, and operational research; infrastructure, environment and organization; concepts, doctrine and collective training; information management and technology; and equipment and support."¹ It will also include an analysis by operational function, a detailed robot taxonomy, and a suggested way forward for robot capability development.

As this book is intended to be an initial compendium of technological concepts for the future Army, Chapter 4 moves into another aspect of no man's land—the highest of high ground. Space plays a vital role in the conduct of land operations, providing everything from imagery and communications to the global positioning system (GPS) and computer networks. It is no longer an environment controlled by a handful of powerful nations. As it becomes ever more crowded with an increasingly diverse range of actors and technologies, space will represent challenges and opportunities to prosecuting the Army way of war. It will be important to have reliable access to all of the key force enhancement capabilities that space offers, and redundancy must be ensured.

Access to space-derived capabilities must be ensured through multiple sources. Those sources might include integral space assets, assets of military partners,

1. From Designing Canada's Army of Tomorrow: http://www.army.forces.gc.ca/CALWC-CGTAC/pubs/armyoftomorrow/DesigningCanadasArmyofTomorrow_full_e.pdf

or even civilian systems. Civilian satellites may offer capability through the purchase of payload space, usage time, or end product information. Satellites may not provide the only solution. Many of the force enhancement areas traditionally associated with satellites may be offered in the future by high-altitude UAVs or similar aircraft. Even ground-based systems figure into a multi-domain solution that ensures redundancy in space capability areas. The chapter on Army access to space provides greater detail and points to some interesting potential uses of space, including target acquisition, support for pervasive networking, and operationally responsive space, where small, inexpensive satellites are launched in temporary orbits to support particular missions.

In a similar fashion, the cyber environment continues to grow at an astonishing pace, serving as the glue which holds modern society together. It keeps critical infrastructure functional, allows for instantaneous transmission of information, and makes global social networking possible. The Army relies on cyber as the backbone of its C4ISR architecture, just as adversaries need it for theirs. The overlapping of friendly, neutral, and adversarial battlespaces creates the potential for conflict, exploitation, and increased vulnerability. The Army will need to understand cyber well if it is to operate successfully in the future.

Chapter 5 will begin by describing the cyber environment, focusing on the physical nature of cyber and the phenomenon of electronic convergence that is expanding the domain where computer network operations (CNO) may be conducted. From there, deterrence and offensive operations concepts will be examined, leading to the conclusion that defence is the critical aspect of cyber, but defence alone cannot deter. In the Army cyber concept, cyber relates to CNO, electronic warfare (EW) and command and control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). Cyber represents the fusion of EW and signals intelligence (SIGINT) with traditional CNO and has several components that fit into the larger C4ISR architecture. However, cyber is not limited to C4ISR; it also plays a vital role in the Act and Shield operational functions.

The electromagnetic world, in the form of the cyber environment, and the lifeless void of space each stand poised to take centre stage in the conduct of land operations. Interestingly, these are places where soldiers will not set foot. There are places on the land, and in the air above that land, where sensing and engagement will be required but where humans may not be needed. Those



spaces will become increasingly crowded with an ever-growing arsenal of unmanned autonomous systems, further expanding the conceptual space known as no man's land.

CHAPTER 2

ROBOTS IN THE ARMY: A STUDY OF UNMANNED SYSTEMS



“You may fly over a land forever; you may bomb it, atomize it, pulverize it and wipe it clean of life—but if you desire to defend it, protect, and keep it for civilization, you must do this on the ground, the way the Roman legions did, by putting your young men in the mud.”

—T.R. Fehrenbach, *This Kind of War*

PART ONE – INTRODUCTION

“You may fly over a land forever; you may bomb it, atomize it, pulverize it and wipe it clean of life—but if you desire to defend it, protect, and keep it for civilization, you must do this on the ground, the way the Roman legions did, by putting your young men in the mud.”²

Unmanned systems are being employed in the prosecution of military operations and are already having significant impact. The use of robotics is a departure from more traditional methods of task execution, and it has greatly enhanced Army methods of intelligence, surveillance and reconnaissance (ISR) and the generation of effects through target acquisition (TA) and remote strike capability. With the exception of certain niche tasks, such as explosive ordnance disposal (EOD), unmanned capability has been mostly restricted to the skies, where a plethora of unmanned aerial vehicle (UAV) systems has extended the range of Army sensing and allowed for ever-increasing levels of standoff. Drawing on the lessons learned from these joint systems, it is now time to conceive the use of unmanned systems wholly generated by the Army in order to gain a better understanding of how they will fit into the Army of Tomorrow and beyond. To that end, this paper will provide a framework for unmanned systems, proffer principles for their employment, and lay down a potential road map for their incorporation into future army concepts. It will show that such systems can enhance the Army of Tomorrow’s ability to disperse and rapidly aggregate because they are able both to provide a presence where humans cannot and to carry out tasks in which humans are not essential for mission success. In the future, humans will still be needed to engage the population, an activity which will be personnel-intensive and unsuited to robots. By leveraging the pervasiveness of the future network, most other tasks, including those that fall under the core functions, may be done by unmanned systems.

1.1 AIM

This study will present the results of CALWC research into unmanned systems in order to provide a framework for robotic systems, principles for their employment, and a road map for incorporating them into future army concepts.

2. T.R. Fehrenbach, *This Kind of War*, 290.

1.2 HISTORICAL PERSPECTIVE

Aerial systems such as Predator and Global Hawk are well known within military circles because of their high degree of success on recent operations. The incorporation of robotics into military affairs is nothing new, however. Though public focus on these systems has steadily grown since the first Gulf War, examples of their employment can be found throughout much of 20th-century conflict. Innovations in breaking the stalemates of trench warfare in World War I included the use of a remote-control land torpedo equipped with wire cutters, explosives, and even missiles.³ Though the land torpedo did not make it off the proverbial drawing board, it serves as an early example of how robotic systems were believed to have the potential to influence ground tactics. During World War II, Goliath, a small remotely operated tracked vehicle packed with explosives, was used by the German Army to defeat advancing Allied tanks on the Atlantic coast via remote detonation.⁴ However, there was limited use of unmanned ground vehicle (UGV) systems in the decades that followed. Though there was some use of UAVs during the Vietnam War, with very minor success, UGV systems do not seem to have been employed during that period. Research and development carried out by the United States Department of Defense (DoD) on unmanned breaching systems in the 1980s met with some success and set the conditions for the employment of robotic EOD and mine clearance systems in the first Gulf War.⁵

Of significant historical importance, however, is the use of UAVs during that particular war. Employed as an ISTAR capability, Gulf War-era UAVs had great success in finding targets. There was even one highly publicized incident in which some Iraqi soldiers surrendered to a UAV by waving white sheets for its remote operators to see, thereby averting the impending destruction it signified. After the Gulf War, the conditions were set for explosive UAV growth in the United States, a trend that would be mirrored—although on a smaller scale—by other militaries. It is useful to take note of trends in the commercial robotic sector as well. Governments often exploit commercial developments because such technologies can be cheaply and readily co-opted for military use. UGVs' application in military operations was largely disregarded until the World Trade Center (WTC) attack of 2001. At Ground

3. Major Gregory J. Nardi, *Autonomy, Unmanned Ground Vehicles, and the US Army: Preparing for the Future by Examining the Past*, School of Advanced Military Studies, USACGSC, Fort Leavenworth, KS, AY 2008–2009. 29 July 2010: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA506181&Location=U2&doc=GetTRDoc.pdf>, 37.

4. Lieutenant Colonel Marcus Fielding, "Robotics in Future Land Warfare," *Australian Army Journal*, 3.2 (Winter 2006): 99. 29 July 2010: http://www.defence.gov.au/army/lwsc/docs/aa_j_winter_2006.pdf; and Nardi, *Autonomy* 37.

5. Nardi, *Autonomy*, 39.

Zero of the WTC, robots were used to great effect in both rescue and recovery operations to search for humans through urban rubble polluted by hazardous and toxic industrial materials (TIMs).⁶ Military planners were quick to see the potential for these devices in the so-called War on Terror that ensued.

1.3 MISSION ANALYSIS


In order to examine the concept of unmanned systems use by the Canadian Army, staff at the Canadian Army Land Warfare Centre conducted a mission analysis on the way ahead. The analysis will not be explored in detail here, but it is worthwhile to mention some of its key elements.

The document, titled *Land Operations 2021: Adaptive Dispersed Operations*, makes it clear that unmanned systems are an enabling concept that requires further consideration. Given the nature of technological change and the successes achieved by other armies in this area, it is now time for a comprehensive look at exactly how unmanned systems will fit into the Army of Tomorrow and beyond. Because unmanned systems encompass such a broad area, mission analysis was a useful tool in narrowing the scope of this examination and in providing logical bounds to the research. Specifically, assumptions and limitations were considered and will be discussed below.

Two significant constraints are worth mentioning. Firstly, this paper will not examine human enhancement technologies. Though significant advances are being made in the testing and fielding of exoskeleton prototypes, an application that one may associate with robots, it should be noted that exoskeletons require an onboard operator and as such cannot be considered an unmanned system. This same logic extends to other forms of robotic human enhancement. A second constraint that will frame this particular study and derived robot concepts is that artificial intelligence (AI) resident on static computing systems (also called “agents” or, colloquially, “bots”) will not be considered. Much like human enhancement in terms of its accelerating technological growth and potential for military application, AI itself is not considered an unmanned system. However, AI can be an important component of an unmanned system and is generally associated with autonomous unmanned systems.

This paper will examine third constraints that could conceivably be employed by the Army. Future collaboration across the CAF will be essential for

6. Daniel Sieberg, “High-Tech ‘Bots’ in Medicine and the Military Are Still in the Model T Stage of Robotic Science,” 2–5.



achieving joint interoperability and developmental efficiency, but this paper will not unilaterally present air or maritime concepts. Given the lack of an overarching concept for the Canadian Armed Forces (CAF) in general, it is assumed that other environments will develop their own concepts and designs. This is not to say that Land Staff should ignore developments in other areas—quite the contrary. As will be demonstrated further on, collaboration across the CAF will be essential for achieving both joint interoperability and developmental efficiency.

Another important assumption concerns terminology. There are no standard definitions relating to unmanned systems in the Army or the CAF as a whole. Unfortunately, there is a dearth of standardization in industry, academia, and within other militaries. Therefore, the assumption will be made that terminology may be borrowed from other sources where it makes sense to do so, as long as such definitions work for Army purposes. As an aid to understanding definitions, a taxonomy for unmanned systems is proposed at Figure 2.1.1.

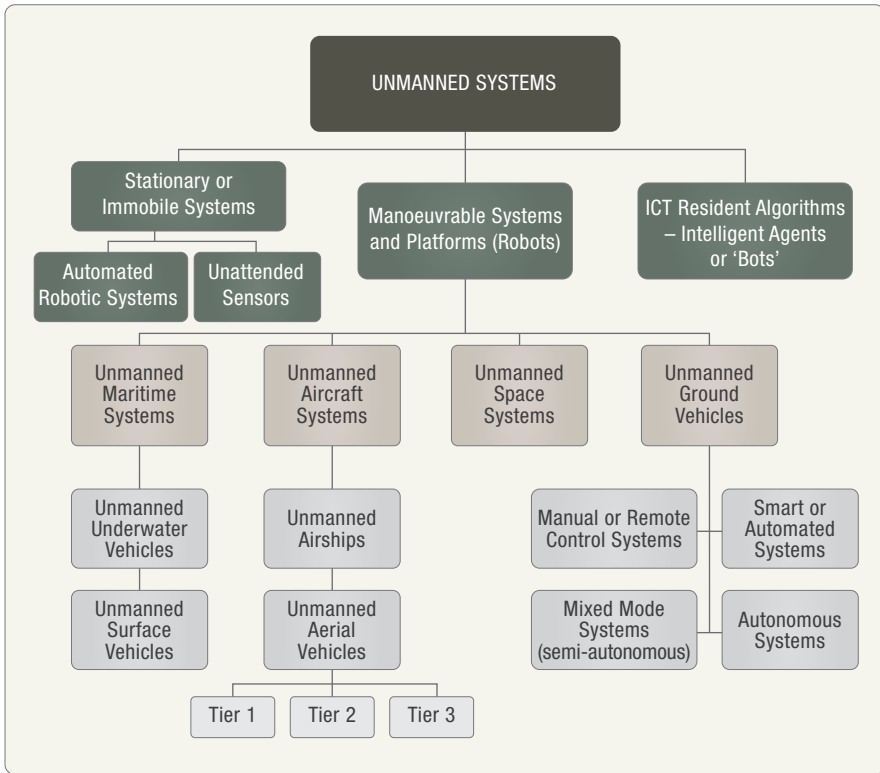


Figure 2.1.1: Unmanned Systems Taxonomy

The following definitions relating to unmanned systems will be used for this study:⁷

7. **Note:** These definitions are not fixed. Initial feedback on this study has led to the development of the following definitions: **Robot.** A robot is an unmanned, reprogrammable, multifunctional mobile platform complete with manipulators, which is designed to move material, parts, tools, or specialized devices through various programmed actions and sense and respond actions for the performance of a variety of tasks in both structured and unstructured environments. Robots are further divided into four sub-classes: (1) **Manual Robots.** A manual robot is a mobile platform that manoeuvres into position and manipulates objects or performs tasks while under manual (remote) control. These robots are commonly called tele-robotic platforms. (2) **Automated Robots.** An automated robot is a mobile platform that manoeuvres into position and manipulates objects in accordance with predetermined programmed input which may or may not be cyclical. These platforms typically operate in structured (familiar) environments. (3) **Autonomous Robots.** An autonomous robot is a mobile platform that manoeuvres into position and manipulates objects within structured and unstructured environments without human operator intervention beyond the initial tasking. Such robotic systems are able to sense their environment, assess the situation, and respond in an appropriate manner within initial tasking parameters. Due to limitations in mobility, dexterity, sensing, and machine intelligence, the range of tasks and environments within which such robots can operate for extended periods without human intervention is currently limited, but it is expected to widen as technology continues to improve. (4) **Mixed-Mode Robots.** Mixed-mode robots comprise function and behaviour features of the aforementioned three robot classes. In practice, this is the most common form of robot in use today, largely due to the abovementioned technical (and cost) constraints that limit the extent to which robots can operate autonomously. Mixed-mode systems are able to move seamlessly between one mode (class) and another and, in practice, are all manual robots that have varying levels of technical sophistication, which allows for varying degrees and duration of automated and autonomous behaviour.

- *Unmanned systems* are electro-mechanical systems with no onboard human operator which are able to exert their power to perform designed missions. They may include platforms such as unmanned ground vehicles (UGVs), unmanned aerial vehicles (UAVs), unmanned underwater vehicles (UUVs), and unmanned surface vehicles (USVs). Unmanned systems include stationary systems such as unattended munitions (UM) and unattended ground sensors (UGSs) incapable of locomotion. Unmanned systems also include artificially intelligent entities or algorithms present on Information and Communications Technologies (ICTs). These systems are often referred to as agents or “bots.” Ballistic projectiles such as missiles, rockets, and their submunitions, and artillery are not considered unmanned systems.⁸ When a system is described as unmanned, that does not mean that human beings are not in the decision or control loop.⁹ It is precisely the unmanned vehicle’s onboard systems, communication links, and interfaces that make it a system rather than simply a vehicle. Those links and interfaces allow the vehicle to receive inputs from a human or from the network itself.
- *Robots* are human-made devices capable of sensing, comprehending, and interacting with their environment. The main parts of a robot are mechanical systems, computers, and sensors.¹⁰ Robots may be regarded as mechanical devices that can be programmed to perform tasks or functions involving movement and manipulation previously performed by humans.¹¹ The distinction between robots and other types of unmanned systems lies in a robot’s ability to manipulate its environment. Robots must also be capable of locomotion in order to move through their environment; therefore, they usually have some sort of uninhabited vehicle component. In this study, the term “robot systems” will also be used. It simply refers to robots and their onboard systems, their operators, and the communications links that connect them all together.
- *Uninhabited (or unmanned) vehicles* can be defined as powered vehicles that do not carry a human operator, can be operated autonomously or

8. Nardi, *Autonomy*, 11.

9. Kenneth Anderson, “Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform,” *Rise of the Drones: Unmanned Systems and the Future of War*, 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136, 2–3.

10. Department of the Army, *Robotics Strategy White Paper*, 19 March 2009, 29 July 2010: <http://www.futurefastforward.com/military-intelligence/1302-robotics-strategy-white-paper-27309>, 5.

11. Fielding, “Robotics,” 100.

remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload.¹² Ballistic or semi-ballistic vehicles, cruise missiles, artillery projectiles, torpedoes, mines, satellites, and unattended sensors (with no form of propulsion) are not considered unmanned vehicles. Unmanned vehicles are the primary component of robot systems.¹³ Key elements of this definition include the lack of a human operator and the requirement for propulsion. Because unmanned vehicles are the primary components of robot systems, they may not form a part of stationary or immobile systems (such as landmines, unattended ground sensors, and coffee makers).¹⁴

- An *unmanned ground vehicle* (UGV) consists of a mobility platform with sensors, computers, software (perception, navigation, learning/adaptation, behaviours and skills, human–robot interaction, and health maintenance), communications, power, and a separate mission package appropriate for its role.¹⁵ UGVs operate on the ground across the range of land-specific environments. Although they do not always take on the appearance of a traditional motor vehicle (some look like animals or even humans), the term “UGV” will be used in this study as synonymous with any robot that operates in the land environment. This definition can be adjusted as the Army moves further through the capability development process.

1.4 ADAPTIVE DISPERSED OPERATIONS

The essence of adaptive dispersed operations (ADO) is to make it possible for widely dispersed teams to conduct coordinated, interdependent, full-spectrum actions across the moral, physical and informational planes of the battlespace, ordered and connected within an operational design created to achieve a desired end state. The fundamentals of dispersed operations, developed from the manoeuvre principles of find, fix, and strike, include the following: developing situations prior to contact; manoeuvring to positions of advantage;

12. Department of Defense (DoD), *Office of the Secretary of Defense Unmanned Systems Roadmap 2007–2032*, 10 December 2007. *Joint Robotics*. 29 July 2010: [http://www.jointrobotics.com/documents/library/Office%20of%20the%20Secretary%20of%20Defense,%20Integrated%20Unmanned%20Systems%20Roadmap%20\(2007-2032\).pdf](http://www.jointrobotics.com/documents/library/Office%20of%20the%20Secretary%20of%20Defense,%20Integrated%20Unmanned%20Systems%20Roadmap%20(2007-2032).pdf), 1.

13. DoD, *Roadmap 2007–2032*, 1; and Nardi, *Autonomy*, 12.

14. A coffee maker is, of course, not a robot. However, it is an unattended, automated system and thus may be considered an unmanned system. See Figure 2.1.1.

15. M. Trentini, D. Purdy, and S. Bogner, *Autonomous Land Systems Applied to Indirect Fire Support 2005–2020: A Technology Assessment, Defence Research and Development Canada*. Technical Report TR 2003-134, November 2003: 9; and Board on Army Science and Technology, *Technology Development for Army Unmanned Ground Vehicles – Summary*, The National Academies, January 2003. *The National Academies Press*. 29 July 2010: http://www.nap.edu/catalog.php?record_id=10592.

influencing the adversary beyond the range of its weapons with lethal and nonlethal capabilities; destroying the enemy, when necessary, with precision and area effects; conducting close engagement, when necessary, at the time and place of own choosing; and transitioning between operations without loss of focus or momentum. These fundamentals are applied across the moral, physical, and informational planes of the battlespace. In short, adaptive dispersed operations call for networked and integrated land manoeuvre forces—supporting and supported by JIMP integrated effects—alternately dispersing and aggregating over extended distances to identify, influence and defeat full-spectrum threats throughout the multidimensional battlespace. Dispersion, in this context, is in terms of time, space, and purpose.¹⁶

Distributed autonomous systems are referred to in the *2021 Force Employment Concept as an enabling concept for the Army of Tomorrow*.¹⁷ Indeed, robots of varying classes and degrees of autonomy can enable ADO in several ways. Developing situations prior to contact by contributing to intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) activities is one way in which unmanned systems can contribute to ADO. Without an onboard human operator, robots are able to access areas previously unreachable by humans. This could include close urban terrain such as tunnels or “rubbled” buildings and areas contaminated by TIMs or CBRN materials. They also offer advantages in terms of time on station and mission endurance. As some writers have put it, a robot can stare at something for days without respite, never blinking. We must be careful, however, not to think of robots as simply unattended sensors. Another key advantage offered by robots is their ability to manoeuvre to positions of advantage. In terms of ISTAR activities, manoeuvre is an essential component because only through mobility can sensing be optimized.

A fundamental of ADO is the ability to influence the adversary beyond the range of its weapons with both lethal and nonlethal capabilities. The implication of this statement is that humans must be beyond the range of enemy weapon systems while at the same time maintaining the ability to influence the enemy from a distance. Influence at a distance is usually thought of in terms of indirect fires and nonlethal influence activities (IA) together contributing to the effects necessary to undermine the enemy’s will and shatter

16. This paragraph is taken from *Land Operations 2021: Adaptive Dispersed Operations – The Force Employment Concept for Canada’s Army of Tomorrow*. Ed. Major Andrew B. Godefroy. Kingston, ON: Department of National Defence, 2007. 29 July 2010: http://www.army.forces.gc.ca/DLCD-DCSFT/specialPubs_e.asp, 18–19.

17. Godefroy (ed.), *Land Operations 2021*, 11.

their cohesion. Robots offer the ability to close with the enemy, to well within its own weapons ranges, while keeping humans at a safe distance. Once it has closed with the enemy, the unmanned system can be employed in just about any manner conceivable to influence the enemy. Similarly, a robot that has closed with an adversary can enable other friendly assets situated beyond effective range of enemy weapon systems to more effectively or efficiently engage the adversary at long range. This idea ties in well with the ADO concept, which acknowledges that sometimes there is a need to physically destroy the enemy. Robots also play a role through direct strike engagement or by enabling other systems in a reconnaissance and target acquisition or find and fix role.

Key to the success of ADO is the ability to know when dispersion or aggregation is required. Once the requirement is known, it will be essential to have the ability to manoeuvre rapidly to a position of advantage so that the desired effects can be brought to bear. As such, maintenance of momentum in transition through efficient enabling operations will be vital. Robots can contribute to enabling operations by allowing more rapid information gathering and processing and by contributing to the overall integration of humans with the network. Simply put, as robots conduct tasks for which humans are not required, the human soldier is given a degree of flexibility and agility to concentrate on those tasks that are exclusively the domain of humans. For example, in a counterinsurgency (COIN) campaign, the primary focus of the Army is on securing the local population. Providing this security will produce the secondary effect of isolating an insurgency from its support base, thereby reducing both the legitimacy of the insurgents and the overall threat they pose. Traditionally, COIN requires tremendous agility in recognizing and responding to different threats. While engaging the adversary, there is the ever-present threat of isolating one's own forces from the local population through psychological effects, civilian casualties, or collateral damage. Robots can be employed to reduce collateral damage and civilian casualties. They can be used in a combat or combat support role in the conduct of offensive or defensive operations, thus either freeing up more human soldiers to continue with engagement of the local population or enabling a quicker fight that allows soldiers to rapidly transition back to conducting stability tasks.

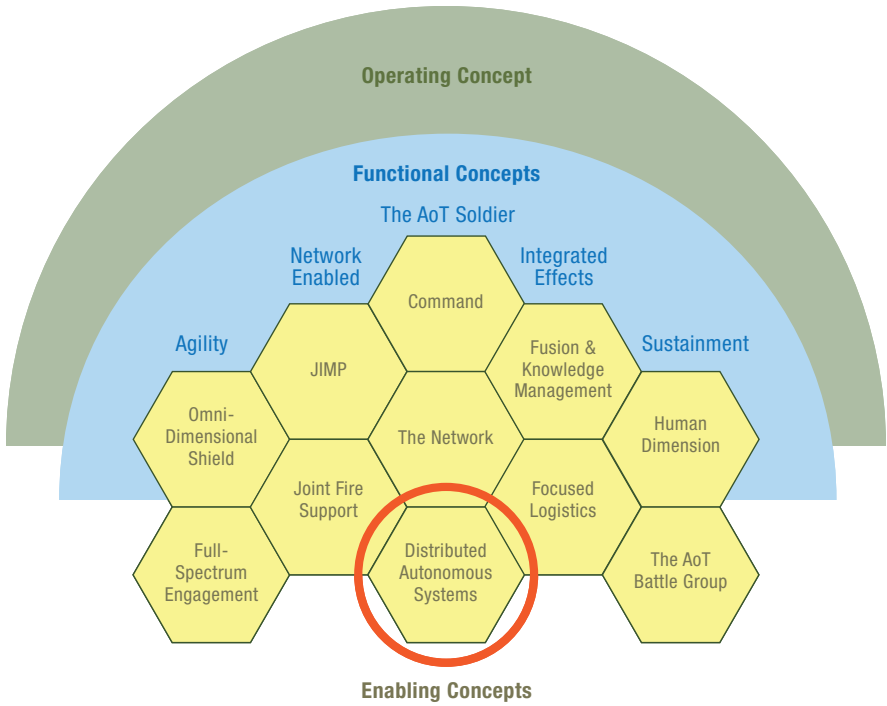


Figure 2.1.2: Adaptive Dispersed Operations

1.5 THE ROBOT REQUIREMENT

As technological change gathers pace, capability planners need to consider the uses and benefits that robots offer the military of tomorrow.¹⁸ Given the overwhelming number of applications that may be offered to the Army by such systems, it is important to evaluate which tasks take priority. An infinite pool of resources for research and development, experimentation, trials and evaluation, acquisition, and lifecycle management is not and will never be available. Therefore it is essential that priorities be identified and measured against technological readiness. In order to identify priorities, the overall requirement for robots must first be identified. Will they be used to close a capability gap in the Army? Capability gaps include roles in which humans cannot function or cannot function optimally. Will they be used to augment the existing capacity of humans? Will they be used to displace (or replace) humans in the conduct of tasks that are dull, dirty, and dangerous? Will they be used to fulfil a moral imperative to do all that we can to protect our

18. Fielding, "Robotics," 99.

soldiers? Undoubtedly, it would be ill-advised to simply procure unmanned technologies every time industry produces a system that can fill a capability gap or improve on an existing capability. Given the present state and projected path of technological development in robotics, it is imperative that the military requirement be defined as soon as possible so that the right systems are developed (or acquired) for incorporation at the right times.

There are a number of capability deficiencies driving the demand to accelerate the introduction of manoeuvrable unmanned systems into the Army. Firstly, there are tasks for which humans are best suited and tasks for which machines are best suited. As long as human soldiers continue to conduct tasks that could be adequately—or in some cases, optimally—performed by robots, an untenable situation will result: there will be insufficient quantities of soldiers to achieve required degrees of human dispersion. Secondly, as units are tasked to conduct information gathering in an ever-expanding battlespace, they will require a mobile sensing capability for those parts of their areas of operation in which humans are not absolutely required and for which they are not well suited. Thirdly, there will be parts of that increasingly large battlespace that will require immediate effects in order to achieve mission success, in which humans will be unable to aggregate quickly enough to do so. Though much more intense analysis and discussion are required at strategic levels, it must be acknowledged that unmanned systems represent a viable means of generating such effects. Lastly, there is no current method of completely removing soldiers from the dangers associated with land combat. Though current experience with unmanned combat aerial vehicles has reduced much of this risk, there is and will continue to be a need for human presence in areas of conflict. However, robots offer several opportunities for further reduction of risk through a number of different applications. Many of them are discussed further on in this study.

The most important of these opportunities for closing gaps pertains to the force employment concept for the Army of Tomorrow. The Army will need robot systems in order to support the ADO concept, as they will contribute to the optimization of scarce human resources by balancing the ratio of tasks done by humans to those done by robots. This will permit the best use of an increasingly strained human resource base, allowing humans to do only those tasks for which unmanned systems are not suited and letting robots do everything else—supporting, watching, and acting when required.¹⁹

19. This assumes that a rigorous cost–benefit analysis is conducted for any given system.

Prevailing ideas for the employment of robots all revolve around the same core themes. Robot systems offer increased survivability and reduced risk to human life and limb through the provision of increased standoff; they offer a tremendous reduction of costs;²⁰ they can eradicate boring and repetitive work (including ISR and logistics tasks) or greatly reduce soldier workloads; they offer increased mission endurance and time on station; they give commanders the ability to take on increased operational risk; they can be exploited to offset personnel shortages; and they offer the potential to change the very nature of military operations. Certainly all of these themes represent areas of great interest for the Army. Therefore, before we can definitively state which tasks we would like to see robots carry out, we must first understand which of these core themes represent Army priorities. Suitable tasks will then emerge from those priorities.

PART TWO – CURRENT CAPABILITIES

In order to provide an overarching concept for the use of unmanned systems within the Army, we need to be aware of the state of military robot employment and of the current state of military, commercial, and industrial robot development. By understanding how robots are currently employed and by looking at where research and development (R&D) is focusing, we can get a better understanding of where robots are headed and of the future potential that robot systems hold. This is an important step in the development of a future robot concept, which, although unbounded intellectually, ultimately must be grounded in reality.

2.1 CANADA

The Army has limited experience with robot systems. Although the Air Force has made tremendous headway in developing and employing UAVs, the Army has not made similar progress on the ground. The situation is consistent with the present state of technology, where advances in the air and maritime

20. Hewitt says, "One of the equipment options being studied for Project CLS 65 is the 'Bobcat Remote Controller'. There are two versions of this kit: version 1 is a straight forward robotic control add-on operated from a 'bellypack' wherein the operator is in direct line of sight and relatively close to the task where the Bobcat is working. There is a basic short-range radio control link, and this assembly is a modest \$12,000. An 'EOD' version uses the same basic control equipment but is enhanced with 8 separate cameras, a robust long-range radio control and data link, plus a sophisticated display allowing complete control without the operator being near to the task, and this comes in at \$120,000. Both versions can be used with almost all Bobcat models of recent manufacture. Of note is the ten-fold increase in cost for control capability not requiring an on site operator. The interesting point here is that this type of technology can turn almost any normal land vehicle in a ROV for between \$12,000 and \$120,000, dependent upon exposure of the operator. This may have huge potential for both cost savings and equipment inventories if 'dual usage' of assets can be achieved." As relayed in Hewitt, "Comments."



domains have greatly outpaced ground-based systems. The reasons for this will be discussed in greater detail in the section on technological limiters in Part Three of this study.

Currently, robot systems generated for the land environment consist mainly of tele-operated EOD robots and small UAV surveillance systems. Other robots in the inventory include CBRN detection systems (such as the Multi Agent Tactical Sentry (MATS) robot employed by the Canadian Armed Forces Joint Incident Response Unit) and landmine detection and clearance systems (such as the Improved Landmine Detection System (ILDS)).

Defence Research and Development Canada (DRDC), the departmental-level science and technology organization, focuses on the R&D of potential technological applications for the CAF (including the Army). It is an active and proactive organization, within its own R&D laboratories, in partnership with other government departments and agencies, with the private sector and with universities within Canada, as well as bilateral and multilateral R&D arrangements with allies and NATO partners.²¹ Canada (through the Department of National Defence) has been a partner in joint activities on autonomous intelligent systems with the United States (through DoD). Private-sector companies in Canada have been awarded Department of National Defence (DND) contracts and sub-contracts through a number of science and technology programs, such as those under the Defence Advanced Research Projects Agency (DARPA).²²

The DRDC Suffield laboratory has been engaged in R&D of unmanned ground vehicles, with a focus on autonomous intelligence, for the past decade. In collaboration with external partners such as the Robotics Institute of Carnegie-Mellon University, Simon Fraser University, the University of Toronto, and McGill University, DRDC Suffield is investigating the use of tactical UGVs to exploit the potential for increasing soldier survivability, lethality and mobility by reducing the risk to personnel and their workloads, and by improving the efficiency of existing tasks.²³

The Autonomous Intelligence Systems (AIS) section at DRDC Suffield has taken the lead in the development of unmanned systems. The original strategic

21. Harold Stocker, *Autonomous Intelligent Systems: Opportunities and Needs for the CAF/DND*, Defence Research and Development Canada. Technical Memorandum TM-2003-004, July 2003.

22. Stocker, *Autonomous Intelligent Systems*.

23. Stocker, *Autonomous Intelligent Systems*.

objectives set out for AIS included developing methods by which robotic systems can measure and sense; developing algorithms, software, and hardware to control robotic response to changing environments; and developing adaptive learning based on collective intelligence.²⁴ Rather than focusing strictly on the development of new platforms, this section concentrated mainly on data fusion research and the development of cooperative, intelligent systems for various platforms.²⁵ The section's objectives have since evolved to include perceiving the environment through sensing and creating world representations; identifying traversable and non-traversable areas; local path planning to avoid obstacles; and long-range navigation and tactical skills. A significant portion of its research is capability-based; thus, it is not tied to any particular platform. The capabilities are largely algorithmic in nature and are implemented as software. The ensemble of capabilities allows a robot to navigate autonomously within a changing environment. Currently, the autonomous capabilities are being applied to UGVs and low-flying UAVs. DRDC Suffield also collaborates with its sister establishments where and when appropriate. Those collaborations include work on UAVs with DRDC Valcartier and on unmanned maritime systems with DRDC Atlantic.²⁶

Despite the intense R&D activities focused on the development of ground-based robot systems, only the EOD community has been significantly impacted to date, at least in an operational sense. Hazardous EOD procedures, which are normally used to deal with the threat posed by unexploded ordnance (UXO) and improvised explosive devices (IEDs), are largely carried out by tele-operated robotic systems. As of 1 July 2010, the existing EOD robot fleet consists of three types: (1) the tEODor, with a total inventory of 58 (six of the original 64 were destroyed in action); (2) the Allen-Vanguard Mark 2D (AV-2D), with a total inventory of 55; and (3) four Dragon Runner™ DR-20s.²⁷ Multiple sizes of EOD vehicles have been required thus far because of the changing nature of the explosive threat.²⁸ In addition, under active procurement under Project 1111 are ten new dismantled IED disposal

24. Stocker, *Autonomous Intelligent Systems*.

25. Stocker, *Autonomous Intelligent Systems*.

26. Greg Broten, DRDC Suffield, first draft feedback.

27. J.T. Hewitt, Directorate of Combat Systems Engineering Management (DCSEM), "Comments on Draft Army Unmanned Systems Study Paper." E-mail to Major J.C. Gash, DLCD, 8 June 2010. Mr Hewitt explains, "It is important to note the [sic] when the above ROVs were procured, no provision was made for attrition in action nor the higher than normal maintenance resulting from multi-year high tempo expeditionary operations. As ROVs are, by concept, intended to be used in hazardous circumstances, attrition is to be expected. Accordingly, new systems must have adequate provision made for the replenishment of action losses without the need to start a new project, which is the case at present."

28. DCSEM, *Explosive Ordnance Disposal*, 5.

operations (DIEDDO) remotely operated vehicle (ROV) systems. The new systems (one controller, two ROVs) are expected to be in service by early to mid-2011 and may also be provided under other new projects; 40 or more systems could eventually be procured.²⁹

Each tEODor system can deploy and fire shotguns, water cannons, and explosively formed water projectiles (shaped charges) in addition to dearmers slugs and chisels. All these “energetic tools” are lethal to humans in the line of fire. The previous CAF EOD ROV replaced by the TEODOR had similar capabilities from its introduction into service in the late 1970s. As the bulk of open source material relating to the use of military robots concerns the ethical and legal considerations associated with armed systems, it is interesting to note that the Army has had armed robots in operational service for at least three decades.³⁰

Although Canada and a number of other western industrialized countries have well-established robotic vehicle science and technology and development programs for robots and robot systems, U.S. spending on such programs dominates the global field.³¹

2.2 UNITED STATES

Robot systems employed by the United States have evolved from primarily remote-operated, single-mission platforms to increasingly autonomous, multi-mission systems. The fielding of increasingly sophisticated reconnaissance, targeting, and weapons delivery technology has enabled unmanned systems not only to participate in shortening the sensor-to-shooter kill chain, but also to complete the chain by delivering precision weapons on target.³² Four mission areas constitute the US Army’s priorities for how robot systems can fill or improve gaps in operational capabilities.³³ Those priorities are (1) reconnaissance and surveillance, both electronic and visual (this is their number one priority applicable to unmanned systems); (2) target identification and designation—the ability to positively identify and precisely locate military targets in real time is a current shortfall with unmanned systems, therefore latency must be reduced and precision for GPS-guided weapons must be

29. Hewitt, “Comments.”

30. Hewitt, “Comments.”

31. Stocker, *Autonomous Intelligent Systems*; and DoD *Roadmap 2007–2032*.

32. Department of Defense. *Office of the Secretary of Defense Unmanned Systems Roadmap 2009–2034*, 29 July 2010: <http://www.acq.osd.mil/psa/docs/UMSIntegratedRoadmap2009.pdf>, xiii.

33. DoD, *Roadmap 2009–2034*, 6.

increased; (3) counter-mine warfare (IEDs are the number one cause of coalition casualties in Operation Iraqi Freedom, and tele-operated robotic systems provide a complementary capability to ground forces and have saved countless lives); and (4) CBRN and explosive (CBRNE) reconnaissance.³⁴

The US Army has further prioritized the following capabilities for unmanned systems research and development: reconnaissance, mine detection, and countermeasures; precision target location and designation; CBRNE reconnaissance, weaponization, and strike; battle management, communications, and data relay; signals intelligence; covert sensor insertion; littoral warfare; and counter-concealment, camouflage, and deception.³⁵

According to Max Boot, the US spends around \$500 billion a year on its military, almost as much as the rest of the world combined. In fact, the US spends more on the research, development, testing and evaluation of new weapons—\$71 billion in 2006—than any other country spends on its entire armed forces.³⁶ The steadily increasing successes with the DARPA Grand Challenge (for example, one challenge involved a race for robot cars, in which competing robots were required to navigate along the roads of an abandoned town, picking out their routes and obeying all traffic rules. The prize was \$1 million) illustrates the present dominance of American research.³⁷ The figures for DoD expenditures on unmanned systems are staggering. For example, the DoD annual budget for development and procurement of unmanned aerial systems increased from \$1.7 billion in fiscal year (FY) 2006 to over \$4.2 billion in FY 2010.³⁸ The total budget allocated for FYs 2007–2013 relating to unmanned systems is more than \$24.3 billion.³⁹

Today, the US operates over 7,000 unmanned systems in the air, ranging from 48-foot-long Predators to micro aerial vehicles that a single soldier can carry in a backpack.⁴⁰ By 2008, the overall inventory of UGVs crossed the 12,000 mark, with the first generation of armed ground robotics arriving that

34. Department of the Army, *Robotics Strategy White Paper*, 6.

35. DoD, *Roadmap 2007–2032*, 21.

36. Max Boot, "The Paradox of Military Technology," *The New Atlantis*. (Fall 2006): 27. 29 July 2010: <http://www.thenewatlantis.com/publications/the-paradox-of-military-technology>.

37. Ben Crispin, "What Killed the Robot Soldier?" *Strange Horizons*. 10 November 2008. 29 July 2010: <http://www.strangehorizons.com/2008/20081110/crispin-a.shtml>.

38. Dyke D. Weatherington, "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform," *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136, 4.

39. DoD, *Roadmap 2007–2032*, 10.

40. P.W. Singer, "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform," *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136.

year as well—and that was just the first generation.⁴¹ The number of robot systems will continue to grow, given that Congress directed the Armed Forces to field unmanned, remotely controlled technology such that, by 2010, one-third of the operational deep strike aircraft of the Armed Forces will be unmanned; and by 2015, one-third of the operational ground combat vehicles of the Armed Forces will be unmanned.⁴² Given the amount of financial and material investment required to realize such a mandate, DoD was tasked with developing an unmanned systems roadmap outlining the pathway that the services will follow with regard to unmanned systems development and fielding. The roadmap is primarily a business strategy to minimize investment risk, prioritize funding, and reduce acquisition costs.⁴³ In other words, the document does not explicitly describe the baseline concept for the employment of unmanned systems. However, it does give a comprehensive picture of specific robots and associated timelines for their integration into the force.

Although much of this ambitious robot strategy has been curtailed over the last year, many elements remain in place. The Pentagon, for example, is pushing ahead with plans for new ground robots such as the Multifunction Utility / Logistics and Equipment (MULE) vehicle, a two-and-a-half-ton truck that could carry supplies into battle or wounded soldiers out of it; the armed robotic vehicle (ARV; not to be confused with the Canadian armoured recovery vehicle), a five-ton mini-tank that could be equipped with missiles or a .30 mm chain gun; and the soldier unmanned ground vehicle (SUGV), a 30-pound, man-portable scout that comes equipped with weapons and sensors.⁴⁴

The SUGV is the most prominent UGV in Iraq. It consists mainly of PacBot and Talon systems—much like the aforementioned World Trade Center robots—that conduct missions ranging from ISTAR and EOD to strike tasks. The ARV has already made its way to Iraq in various forms, including the iRobot Warrior and the Foster–Miller modular advanced armed robotic system (MAARS). On 4 June 2008, the first MAARS unit was shipped to Iraq for testing in the field. A year later, iRobot deployed its armed Warrior to the battlefield.⁴⁵

41. P.W. Singer, "Wired for War? Robots and Military Doctrine." *Joint Force Quarterly*, 52.1 (2009): 105. 29 July 2010: http://www.brookings.edu/articles/2009/winter_wired_singer.aspx.

42. Department of the Army, *Robotics Strategy White Paper*, 7. With the cancellation of the Future Combat Systems project, the achievement of these goals may be in doubt.

43. Nardi, *Autonomy*, 45.

44. Boot, "The Paradox," 25.

45. Crispin, "What Killed."

Meanwhile, the mobile detection assessment and response (MDARS) program has successfully fielded the first semi-autonomous ground robot for use by DoD. The MDARS exterior patrol unit vehicle is an advanced UGV employed by logistics forces and is capable of self-guided navigation using differential GPS and inertial sensors, along with light detection and ranging (LIDAR)-based obstacle detection and avoidance capabilities, to autonomously patrol high-value storage facilities.⁴⁶

One example of the 7,000 unmanned aerial systems presently deployed is the multi-mission MQ-9 Reaper. This UAS, which is larger than the Predator, has an ordnance payload of up to four GBU-12 laser-guided 500-pound bombs or fourteen Hellfire missiles.⁴⁷ George Johnson, the leader of the robotics program at the Pentagon's Joint Forces Command Center, recently told reporters asking about autonomous robots, "the American Military will have these kinds of robots. It's not a question of if; it's a question of when."⁴⁸

2.3 OTHER DEVELOPMENTS OF INTEREST

In general, US capabilities in both research and technology fielding are leading the way internationally. Canada's efforts may be considered comparable to those of the US in terms of platform technology, albeit on a far smaller scale. Beyond North America, significant research is being conducted in Germany, Australia, France, the UK, Israel, South Korea, Switzerland, Denmark, Japan, and China.⁴⁹ Japan's efforts in human robot interface research are comparable to those of the US. The United States presently shares R&D information on unmanned systems with the United Kingdom, Australia, Sweden, France, Israel, Germany, Canada, Singapore, Norway, Italy, Japan, and South Korea.⁵⁰

R&D is truly an international effort that goes beyond military interests. At least 40 other countries are currently developing unmanned systems technology—including Iran, Russia, and China. During the Israel-Lebanon war in 2006, Hezbollah deployed three surveillance UAVs that it acquired from Iran. A survey of *Jane's Defence Weekly* or the *Federation of American*

46. Hoa G. Nguyen et al., "Land, Sea, and Air Unmanned Systems Research and Development at SPAWAR Systems Center Pacific," *SPIE Proc.* 7332: Unmanned Systems Technology XI, Orlando, FL, April 14–17, 2009. 29 July 2010: <http://spiedl.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf&id=PSISDG00733200000173321000001&idtype=cvips&prog=normal>, 7.

47. Samuel N. Deputy, *Counterinsurgency and Robots: Will the Means Undermine the Ends?* Paper submitted to the Faculty of the Naval War College, Newport RI, 04 May 2009. DTIC. 29 July 2010: <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA503005>, 3.

48. Crispin, "What Killed."

49. DoD, *Roadmap 2007–2032*, 55.

50. DoD, *Roadmap 2007–2032*, 56.

Scientists website reveals the global extent of robot development and employment. Countries with academic, commercial, industrial, or military robot programs are depicted in Figure 2.2.3.

PART THREE – TECHNOLOGICAL READINESS

The idea of technological readiness for military robots extends well beyond any one platform technology. To be sure, the importance of mobility technologies cannot be overstated, but there are many other areas of technological development that are essential for robot functionality. Of interest to the military capability development community are the many great advances in fields related to robot systems. These include, for example, advances in novel and strengthened materials, miniaturization (in the form of micro electro-mechanical systems (MEMS)), nanotechnology, sensor technology, radar, computing power, logic, biotechnology, lasers, communications, satellite technology, and myriad other scientific and engineering disciplines.⁵¹

It seems likely that microprocessors in the year 2020 will approach the data processing capabilities of the human brain. Most academic scientific models indicate that technology can be predicted only up to ten years in advance. Therefore, the capability of future unmanned systems is difficult to imagine.⁵² Some experts agree that the speed of technology is moving so fast that the world as we know it may be subjugated to an event horizon.⁵³ Often expressed as the “singularity,” this is the point where machine intelligence overtakes human intelligence, thus placing humanity on an irreversible course of machine-engineered evolution where the bulk of cognitive power will rest with artificially intelligent agents. The concept of computers doing almost everything that is intellectually challenging certainly has powerful implications regarding the future of warfare.⁵⁴ Needless to say, the exponential increases in computing power will allow for the development and employment of ever-increasing levels of robot autonomy. A higher level of autonomous operation is certainly desirable for many systems; however, it is unlikely that full autonomy will be advantageous for many systems. This will be discussed further below.

51. Stocker, *Autonomous Intelligent Systems*.

52. Erin A. McDaniel, *Robot Wars: Legal and ethical dilemmas of using unmanned robotic systems in 21st century warfare and beyond*, Thesis presented to Faculty of US Army Command and General Staff College, Fort Leavenworth, Kansas. 2008. 29 July 2010: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA502401&Location=U2&doc=GetTRDoc.pdf>, 48.

53. McDaniel, *Robot Wars*, 71.

54. McDaniel, *Robot Wars*, 72.

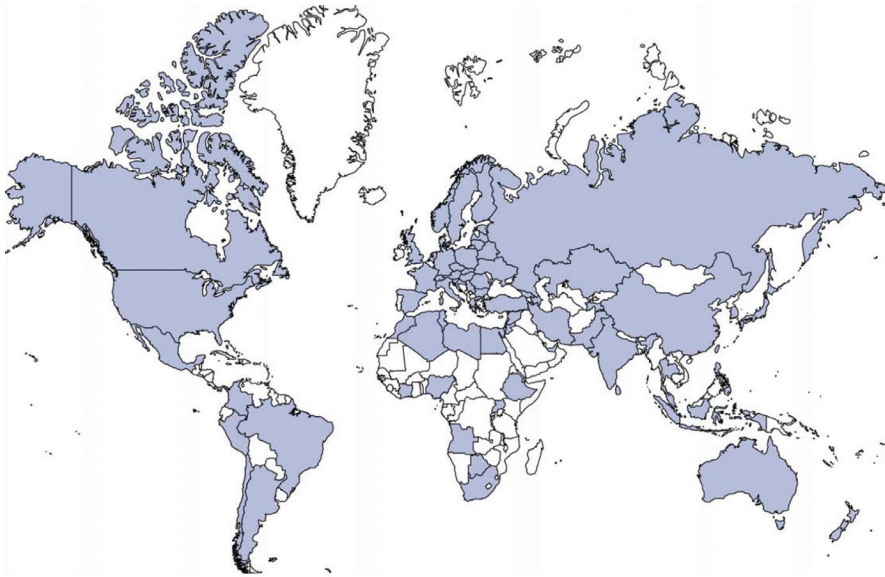


Figure 2.2.3: Countries Developing Unmanned Systems Technologies

As machines are imbued with human levels of intelligence, it is hoped that future robots will be capable of discriminating reliably between civilian and military entities. This has even led a number of critics to argue that the use of robots as autonomous weapon systems is actually morally superior.⁵⁵ They argue that future autonomous systems will be able to abide by the current laws of warfare and rules of engagement significantly better than humans due to several advantages. Those advantages include enhanced sensors used for superior battlefield observation and lethal engagement; the elimination of counterproductive human emotions such as fear, anger, and guilt, which may lead to war crimes; the ability to report criminal activity committed by soldiers; the ability to accurately record and monitor human ethical behaviour during routine combat operations; the ability to maintain superior battlefield momentum as a result of the inability to experience mental or physical exhaustion; the inability to think about self-preservation and the ability to self-sacrifice; and, lastly, the capacity to react with lethal force more accurately and more quickly than any human soldier.⁵⁶

55. Ronald C. Arkin et al., *Responsibility and Lethality for Unmanned systems: Ethical Pre-mission Responsibility Advisement*, Technical Report GIT-GVU-09-01, Georgia Institute of Technology, 29 July 2010: <http://www.cc.gatech.edu/~alanwags/pubs/GVU-TR-09-01.pdf>, 1; and Robert Sparrow, "Killer Robots," *Journal of Applied Philosophy*, 24.1 (2007): 70, 29 July 2010: <http://www.sevenhorizons.org/docs/SparrowKillerRobots.pdf>.

56. McDaniel, *Robot Wars*, 29.

Although some argue that it will become increasingly difficult to leave the human in the loop because of the high number of decisions that will be required and the pace at which those decisions must be made, it is doubtful that machines will ever be smart enough to do all of the fighting, even if they can perform some of the duller, dirtier, or most dangerous work.⁵⁷ The Hollywood movies *Terminator* and *iRobot* both depicted humanoid-like robots with highly advanced artificial intelligence (AI) capabilities that unquestionably exceed current technology, probably by hundreds of years.⁵⁸ The reality of fully autonomous weaponized UGVs which can distinguish enemy combatants and attack them without direct human control remains several decades away.⁵⁹ The establishment of a climate of trust between humans and unmanned systems over the next fifteen years will be required before any decision can be made about integrating fully autonomous systems into the Army, beyond basic ISR or logistics systems.

3.1 TECHNOLOGICAL LIMITERS

Widespread applications of ground-based robot systems have been limited due to the level of task complexity and the nature of the operational environment, required computing power, and integration of sensors and perception technologies required to perform more dynamic missions.⁶⁰ There are two chief technological limitations on the use of robots at the moment. First, computers and sensors are not yet smart enough to deliver anything close to the situational awareness that can be achieved by a human being. Second, a shortage of bandwidth limits the number of systems that can be remotely controlled at any one time.⁶¹ More specifically, there are many potential showstoppers for developing UGV systems. These potential showstoppers are presented, roughly in order of significance, in the bulleted paragraphs that follow.

- *Perception (on- and off-road) and World Representation*—Complex and unstructured ground environments pose significant perception challenges. A robot's inability to understand its environment is the primary reason for lack of performance in the land environment to

57. McDaniel, *Robot Wars*, 64; and Boot, "The Paradox," 26.

58. McDaniel, *Robot Wars*, 52.

59. N.S. Makin, *Future Warfare or Future Folly? Autonomous Weapon Systems on the Future Battlefield: An Assessment of Ethical and Legal Implications in Their Potential Use*. Master of Defence Studies Research Project. Canadian Forces College JCSF 34. 25 April 2008. 12 April 2010: <http://www.CAFc.forces.gc.ca/papers/csc/csc34/mds/makin.doc>, 31.

60. Department of the Army, *Robotics Strategy White Paper*, 5.

61. Boot, "The Paradox," 26.

date. In contrast, UAVs, operating in obstacle- and hazard-free environments, have been used to great effect. There are many situations in which UGV performance is not at the level of a human driver, including complex interchanges, construction zones, driving on snow-covered roads (nearly impossible), driving into the sun at low sun angles, and driving in precipitation (heavy rain, snow, or fog), in dust or in the presence of battlefield obscurants. Signs and traffic signals can be segmented and read only if they conform to rigidly defined specifications and if they occupy a sufficiently large portion of the image. Pedestrian detection remains a problem. A high probability of detection is accompanied by a high rate of false positives.⁶² Tremendous accuracy and precision of image and graphics processing are needed in order to make positive identification for the use of lethal force, and both are even harder to get when movement is involved.⁶³ Present-day technology is sufficient for gathering appropriate depth map data; however, the challenge lies in the accumulation of depth data as the robot moves. The problem is of combinatorial complexity, and thus will likely not be solved by ongoing advances in conventional computing.⁶⁴ All robot systems, except for the smallest special-purpose vehicles, must have the ability to autonomously avoid obstacles. Some combination of radar, optical, and infrared (IR) sensors will likely be required, and image-processing algorithms, especially for the latter two, are still in their infancy.⁶⁵ Human presence detection (HPD) is another area of concern associated with perception technologies. The US HPD project is attempting to increase the ability of UGVs to detect and localize humans while moving, both for tactical purposes as well as for safe robot navigation when operating in proximity to humans. The large-vehicle portion of the project is using LIDAR and radar systems to detect people during vehicle motion, while the small-vehicle portion of the project pursues the use of low-cost monocular and stereo thermal and colour imagery in conjunction with image-processing algorithms.⁶⁶ Again, the closer researchers get to being able to consistently detect human presence, the higher the false positive rate. False positives represent a significant challenge to useful manoeuvrability.

62. Trentini et al., *Autonomous Land Systems*, 31.

63. Crispin, "What Killed."

64. Patrick Chisan Hew, *The Generation of Situational Awareness within Autonomous Systems – A Near to Mid Term Study – Issues*. DSTO-GD-0467, Australian Government Department of Defence – Defence Science and Technology Organization, 29 July 2010: <http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/4560/1/DSTO-GD-0467.PR.pdf>, 6.

65. DoD, *Roadmap 2007–2032*, 51.

66. Nguyen et al., "Land, Sea, and Air," 6.

- *Pose and Localization*—A manoeuvrable unmanned system must simultaneously know its current pose, the route it followed to achieve its current position, the co-ordinates of the desired destinations and where objects of interest are located. Relying solely on GPS for the pose is dangerous, as GPS signals are weak and easily jammed. The Russian company *Aviaconversia*, for example, offers a four-watt GPS jammer commercially for less than \$4,000. Some observers believe that jammers effective over ten-mile radiuses can be built for \$400 from parts available at retail electronics stores. Modern forces are poorly equipped even to identify the existence of jamming.⁶⁷ This gap is likely to be more pronounced if the vehicle operator does not reside at the system's physical location. Given the weaknesses of GPS systems, it is imperative that a robot system have alternative means of estimating its pose that reduce the reliance on GPS. Promising research techniques include visual odometry, various implementations of simultaneous localization and mapping (SLAM) and place-recognition techniques.
- *Tactical Behaviour and Skills*—A UGV must be able to learn by adjusting its knowledge base of tactical behaviours as it experiences repeatable enemy actions or other learning events. Technologies for UGV tactical behaviours and skills are still in their infancy. Modules that can enable complex tactical behaviours, such as difficult terrain negotiations or stealthy operations, will not be developed in the near term.⁶⁸ The development of a UGV that can move using folds in terrain and thick vegetation for cover and concealment, gain and maintain contact with an enemy entity without being detected, and occupy static positions that provide optimal line of sight for communications or for engaging the enemy will not be a reality for the Army of Tomorrow.⁶⁹ It may therefore be concluded that UGVs capable of complex adaptive behaviours are far from reality.⁷⁰
- *Operational Security*—UGVs exhibit fairly easily detectable acoustic, thermal, visual, and communication signatures. In the future, robots will be asked to carry out missions covertly, therefore low signature management attributes will be desirable.⁷¹ Passive signatures (for

67. John A. Gentry, "Doomed to Fail: America's Blind Faith in Military Technology," *Parameters* (Winter 2002–2003): 91. 29 July 2010: <http://www.comw.org/rma/fulltext/0212gentry.pdf>.

68. Trentini et al., *Autonomous Land Systems*, 31.

69. Trentini et al., *Autonomous Land Systems*, 14.

70. Board on Army Science and Technology, *Technology Development*.

71. DoD, *Roadmap 2009–2034*, 27.

example, acoustic target strength and radar cross section) seem amenable to reduction through application of novel materials, construction, or shaping. Active signatures (for example, engine noise and infrared plume) primarily require source-level reductions. Little or no work has been done to apply this technology to improve the stealth of small or medium-sized robots in order to overcome detection sensors such as radar, metal, or IR. Stealth technologies for UGVs are at high risk.⁷²

- *Health Maintenance*—Much of the R&D work to date on health maintenance has been theoretical and may not be easily transferred to practical military systems.⁷³ Other than complexity of the task environment, the principal factor limiting the degree of autonomy of robotic systems remains the reliability of the system, often expressed as mean time between failures.⁷⁴ The electro-mechanical reliability aspect is an engineering issue that can be solved. From the complex systems of system perspective, there are software issues that will present major challenges if robot systems are to be made to operate over extended periods of time.
- *Size, Power, and Energy*—UGVs are available in a variety of sizes. Small platforms have the advantages of a low profile (more stealth) and access to indoor areas, and they can be man-portable. Small robots present unique challenges that the larger systems do not, including severe size, power, and weight constraints. Batteries in robot systems do not last forever; currently, a typical UGV battery lasts about two hours. Batteries are one of technology's great underachievers (the US Department of Energy is reportedly spending billions on battery research).⁷⁵ The present dilemma is that longer endurance requires more power, which in turn requires larger resident platforms for power generation systems. Most of the larger systems currently use sensors that cannot be supported on the man-portable robots, and similar sensors that meet the size, weight, and power requirements of small robots do not provide comparable quality of data.⁷⁶ This is also called the power dilemma: the more sensors required on a particular platform, the larger the platform required, which in turn generates the need for more power. Additionally,

72. Trentini et al., *Autonomous Land Systems*, 31.

73. Trentini et al., *Autonomous Land Systems*, 31.

74. Department of the Army, *Robotics Strategy White Paper*, 6.

75. William Finn, "Don't believe the bunny: Power and unmanned systems," *Amrel*, 2 March 2010. 29 July 2010: <http://www.commoncontrolnow.com/download/Dont-Believe-the-Bunny-Power-and-Unmanned-Systems-Discussion.pdf>.

76. Nguyen et al., "Land, Sea, and Air," 2.

a small platform places more demands on the perception system, since even small objects may represent obstacles. Perception, in turn, demands more processing capabilities and exacerbates the power dilemma. Batteries may not be the answer. Alternative energy sources, including existing technologies such as onboard internal combustion engines, may well be the way ahead. Much more research is required in order to develop optimal power sources for UGVs.



Source: Combat Camera

- *Communications*—Tele-operated robots consume significant amounts of communications bandwidth because they require transmission of control signals and large amounts of sensor data. Line-of-sight (LOS) limitations often obstruct digital radio communications. In addition, encryption, which is necessary for security, can decrease operational distance. Besides compromising range, radio noise may also affect how the robots respond to instructions, even instigating false commands. Another consideration is the additional power consumption necessary to burst through interference. Operational distance may be affected by landscape features, such as hills, hardened concrete walls (a major urban consideration) and friendly jamming.⁷⁷ Autonomous systems can help alleviate the communications bottleneck by enabling onboard decisions, thus reducing the communication volumes between the operator and the UGV.

77. William Finn, "Radio Control and Unmanned Systems," *Amrel*, 16 February 2010, 29 July 2010: <http://www.commoncontrolnow.com/download/Radio-Control-and-Unmanned-Systems-Overview.pdf>.

- *Cooperative Robot Behaviours*—Most of the systems currently developed are not yet able to perform beyond laboratory experiments. Although the potential of large numbers of robot modules has been demonstrated in simulation, implementations involving more than a dozen or so physical modules are still uncommon.⁷⁸

Jared Giesbrecht is a defence scientist working in the AIS Section at DRDC Suffield. He has summarized the major technological limiters facing the land-based robot R&D community as follows:

- Communications.
- Mobility: a soldier can easily step over a three-foot mud wall but currently no robot can.
- Reliability: most of the systems that exist now are run by researchers and engineers. They are complex and fragile. This applies even to many commercial systems. This is to say nothing of how fragile they would be once you started shooting at them—especially their sensors.
- Autonomy: the current level of autonomy needs to progress before robots will be generally useful. Current robot systems have a very high “pester rate,” meaning that they place very high demands on the time and attention of the user—not very useful in a combat situation.
- Utility: most current robots are useful for specific roles (i.e., ILDS or MATS). When taken outside of those applications, they fail miserably. Moreover, a lot of robot systems are not very user friendly, which limits their use (again, who wants to fiddle with something when they are under fire?).
- Cost: for example, the Convoy Active Safety Technology (an autonomous convoying system developed by the US Army’s Tank and Automotive Research, Development, and Engineering Centre) has reached a very high technology readiness level. However, it has not been adopted by the US military in general. It is simply too expensive.

78. Trentini et al., *Autonomous Land Systems*, 31.

PART FOUR – INSTITUTIONAL CHALLENGES

One factor that can influence success in the incorporation of robots into military operations is cohesion between the R&D community and its defence partners. In other words, the science and technology (S&T) push by the R&D community must be matched by defence customer pull, that is, by an operational requirement. Visioning by a military service of its future needs, in isolation and without knowledge of the multitude of today's current and emerging technological advances, will be difficult and much less than optimal. Hence the obligation for the S&T community to inform the military about current and emerging technologies.⁷⁹ The maintenance of this relationship is an institutional challenge.

Institutional challenges are impediments to advancement that will not be necessarily overcome by the passage of time alone. Whereas technological limiters will be overcome—it is simply a question of when—institutional challenges require human will to surmount. Any institutional challenge, whether it is glacially paced procurement systems or fear of change, can largely be overcome through the process of socialization.

4.1 SOCIALIZATION OF THE ARMY TO ROBOT SYSTEMS

Military robotics is a revolution that has already been thirty years in the making.⁸⁰ Despite that fact, robot systems are generally regarded as a futuristic military capability. The few systems that have already found their way into land operations are largely not viewed as revolutionary, since they have already been integrated into the human experience by the proliferation of civilian technologies such as radio-controlled airplanes and police bomb-disposal robots. Given the recent successes of UAVs in military operations, there will be a concomitant demand for similar UGV capabilities. This demand will no doubt yield a mass influx of robotic technologies. Therefore, there is a need to socialize the Army to this influx.

With all new military technology, a socialization process must occur before it is accepted. Socialization, which is not a military process but rather a human process, is the adoption of behaviour patterns of the surrounding culture (the

79. Stocker, *Autonomous Intelligent Systems*.

80. Institut für Religion und Frieden. *Interview with Armin Krishnan*. 23 November 2009. 29 July 2010: http://www.irf.ac.at/index.php?option=com_content&task=view&id=306&Itemid=1.

majority) by an individual or minority group.⁸¹ This normally refers to the process by which an individual learns to adapt to the social climate that pervades an organization, thereby becoming socialized to the larger group. In the case of technology, it is the group itself that must learn acceptance. In the context of robotics, socialization is the process by which soldiers accept novel technology to the point where they insist on integrating it into the conduct of operations. They do not work around it and they do not learn to live with it—they are socialized to want it.



Source: Combat Camera

There are many reasons why technology might not be readily accepted for use in military operations. “Throughout history, nations have attempted to lawfully restrict technological advances in weapon systems. This has occurred since at least 1139 when the Lateran Council attempted to outlaw the crossbow. The underlying reasons for such restrictions were rooted in a sense of chivalry.”⁸² In other words, technology has historically enabled humans to lay greater

81. See Free Dictionary at <http://www.thefreedictionary.com/socialization>.
82. McDaniel, *Robot Wars*, 75.

waste to their adversaries while at the same time affording them greater levels of standoff protection. In some archaic interpretation of the law of war, one might look at technology as the loaded handgun that a schoolyard bully brings to an after-school fight—anything but chivalrous. In terms of robotics, questions remain concerning the law of war and the notion of chivalry. However, it is primarily fear of the unknown that makes human beings unwilling to accept robotic technology. That fear is not grounded in reality.

4.2 FEAR

The future face of technology cannot be divined. When attempting to envision what the future might look like, people are unavoidably biased by any realistic accounts to which they have been exposed. Most societies conceptualize the future based on years of typical science-fiction fantasies with robots portrayed as humanoid-like machines that become independent, self-determining entities seeking to establish their own society or to eliminate humankind.⁸³ Robotist Noel Sharkey even speaks of a ‘threat to humanity.’⁸⁴ Could robots conceivably be turned against their original operators?⁸⁵ Questions like these have already sparked global debates via social-networking media about the employment of current robotic systems in military operations, despite the fact that there are no self-determining robots in existence today that pose a threat to humankind.

Just after the tele-operated weaponized robot known as SWORDS (special weapons observation reconnaissance detection system) was deployed to Iraq by the US Army, accounts began to surface that the robot was not acting as it was programmed to do. Executives talked of signal delays hampering remote-controlled operation, and the SWORDS program manager himself told the media that kill switches were now a feature of the robot, allowing soldiers to “kill the unit if it goes crazy.”⁸⁶ Though all technologies experience setbacks on the way from initial to final operating capability—and sometimes beyond—and kill switches are featured on everything from snowmobiles to lawnmowers, associating these things with armed robots has created undue fear simply because the military has not yet been socialized to robots.

83. McDaniel, *Robot Wars*, 19.

84. Armin Krishnan, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Burlington, VT: Ashgate Publishing Company, 2009), 4.

85. Fielding, “Robotics,” 106.

86. Crispin, “What Killed.”

The development of the V-22 Osprey aircraft has been completely unaffected by the fact that thirty people have been killed during testing.⁸⁷ People are socialized to aircraft technology, so they are not afraid of new aircraft. Indeed, that socialization has contributed to the success of UAVs in recent military operations. Fear of ground-based robots arises not only out of Hollywood humanoid science fiction but also out of military experience with AI setbacks.⁸⁸

Daniel Wilson writes in his humorous book *How to Survive a Robot Uprising*, “If popular culture has taught us anything, it is that someday mankind must face and destroy the growing robot menace.”⁸⁹ Killer robots, in the sense of lethal autonomous military robots, do not exist. Today’s military robots are largely remote-controlled machines, which in rare cases carry weapons. They have no brains to speak of and are highly dependent on human operators for carrying out their narrow functions, which are mainly reconnaissance, explosive ordnance disposal, logistics (mainly warehouse robots), and base security.⁹⁰ We cannot allow our development of robotics to be limited by ethical dilemmas that are based on science fictional fear which is in turn based on artificial Hollywood portrayals of robots run amok.⁹¹ However, as robot technology continues to improve, we must remember that giving a machine the complete authority to eliminate human life significantly changes the foundations of our existence.⁹² Accepting this fact is one thing. Using it as an argument to restrict the development of other unmanned systems is quite another.

4.3 LEADERSHIP RESPONSIBILITY

Soldiers will not accept robot systems technology if military leaders do not actively encourage their acceptance. In order to integrate radical new technologies and concepts, changes in established procedures and work are

87. Crispin, “What Killed.”

88. In 1988, the missile cruiser USS Vincennes was fresh off an exercise simulation of an F-14 attack just prior to the ship’s deployment to the Mediterranean. What the ship’s crew did not know was that the simulation had not been properly reset. During the actual deployment, a skirmish took place with a number of Iranian speedboats. The quantity of speedboats could potentially have overwhelmed the crew’s ability to engage in a timely fashion; therefore, a decision was made to activate the ship’s autonomous defence system. The ship’s radar system subsequently detected the speedboats and even detected an inbound Iranian F-14 aircraft. The aircraft was identified by the system as hostile, attacked by fire and immediately destroyed. Later, it was determined that the aircraft was actually a civilian Iranian passenger jet carrying roughly 290 passengers which had presented as an F-14 due to the fact that the simulation had not been properly reset. Human memories associated with this type of incident will certainly undermine attempts to socialize the future force to robotic weapons. See McDaniel, *Robot Wars*, 42.

89. Krishnan, *Killer Robots*, 1.

90. Krishnan, *Killer Robots*, 1.

91. Thomas H. Cowan, *Theoretical, Legal and Ethical Impact of Robots on Warfare*, USAWC Strategy Research Project, US Army War College: Carlisle Barracks, PA. DTIC. 29 July 2010: <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA469591>, 12.

92. McDaniel, *Robot Wars*, 20.

required, and that will always elicit resistance.⁹³ Leaders will be responsible for ensuring that fear of the unknown is transformed into an embracing of robots' potential. Within the Army, the culture of soldiers and their leaders will impact the acceptance of robots, especially if robot systems are portrayed as replacing soldiers rather than enhancing a soldier's capabilities or displacing a soldier from harm's way.⁹⁴

Beyond acceptance at the tactical level, leaders at the strategic level must also embrace the potential of robotic solutions to military problems. If success is to be ensured throughout the capability development process, challenging technical goals can only be set if the command structure recognizes and accepts the potential value of these systems, embraces the need for them and demands a high level of reliability and performance from their developers.⁹⁵

4.4 BUILD ON EXPERIENCE

Outside of military operations, there are numerous instances of successful robot application. They include crawling through collapsed buildings looking for 9/11 survivors, helping locate lost mountain climbers, and serving as terrestrial rovers on Mars, to name just a few. The attention such systems have received in the news media increases public acceptance of them.⁹⁶ On operations, a number of bomb-clearing devices have been nominated for medals by their human colleagues. One, the property of the 737th Ordnance Company (US Army), was promoted by its fellow soldiers to the rank of Staff Sergeant. "Sgt TALON" has also received three Purple Hearts.⁹⁷

Opportunities must be exploited to build on positive robotic experiences that can shape attitudes governing the acceptance of future robot applications. The US Unmanned Systems Integrated Roadmap discusses the positive reputations of robot systems. UAVs continue to improve on their reputation as a reliable and invaluable contributor to land operations as evidenced by land commanders' almost insatiable need for full-motion video and ISR information.⁹⁸ UAVs have saved countless lives by providing evidence of IEDs planted on convoy routes, warning troops of ambushes, assisting troops in

93. Leighton Hanon, *Robots on the Battlefield – Are We Ready For Them?* American Institute of Aeronautics and Astronautics, Inc. Chicago, IL, September 2004, 29 July 2010: http://pdf.aiaa.org/preview/CDReadyMUAV2004_1007/PV2004_6409.pdf, 3.

94. Nardi, *Autonomy*, 31.

95. Hanon, *Robots on the Battlefield*, 10.

96. DoD, *Roadmap 2007–2032*, 48.

97. Crispin, "What Killed."

98. DoD, *Roadmap 2009–2034*, 37.

contact, and permanently removing high-value assets from the battle. Similarly, the employment of UGVs to detect, interrogate, and defeat IEDs has benefited soldiers enormously, with approximately 12,000 UGV operations per year and the prevention of thousands of casualties.⁹⁹ These baseline successes can frame the future path of robot integration in a positive manner.

The Army can draw on the successes of other nations, but it will be through our own process of socialization that we will gain acceptance of robots and insist on their application in an ever-widening range of scenarios.

4.5 ENSURE USER-FRIENDLINESS

Ease of operation allowing a straightforward integration of robot systems will be essential for the socialization process. All new systems face operator distrust or a so-called “show me” attitude. If these systems are easy to use—familiar and reliable—they will be more easily accepted. If not, they will be shunted aside or operators will hunt for problems as an excuse to avoid using the systems.¹⁰⁰ The Army experience with the adoption of digitization tools provides a useful analogy, demonstrating the importance of user-friendliness in ensuring technological acceptance.

Any technological design that contributes to ease of operation will assist the acceptance process. Insisting on common control stations and simplistic human robot interfaces are techniques that will add to successful integration. The pursuit of steadily increasing degrees of autonomy for robotic technologies—keeping humans in the loop—will also contribute. Semi-autonomous operation allows a robot to operate without human intervention until certain critical decision points are reached.¹⁰¹ Semi-autonomous robots equipped with the ability to make simple decisions (for example, left or right around an obstacle) will make operation significantly easier for human controllers, who need be prompted for decisions only when those decisions have mission-related consequences. Increasing levels of autonomy contribute proportionally to an overall reduction in the operator’s workload.

99. DoD, *Roadmap 2009–2034*, 37.
100. Hanon, *Robots on the Battlefield*, 3.
101. McDaniel, *Robot Wars*, 3.

4.6 DEMONSTRATIONS

Demonstrations of robot prototypes can assist in socializing troops to unmanned systems. Soldiers are more likely to accept new technologies if they witness effective field demonstrations. NATO, for example, through IST-089 (Information Systems and Technology), supports periodic demonstrations via the European Land Robotics (ELROB) Trials, where robots are demonstrated under realistic conditions. Beyond simple military or corporate demos for capability developers, another method of encouraging acceptance is to create a robotic pool that gives field units a chance to experiment with future robotic systems.¹⁰² Such a pool would need to be supported by a competent project team responsible for ensuring that good ideas are acted upon in a coherent and timely manner and bad ideas are recorded and avoided in future projects.¹⁰³

4.7 NOTE ON DISRUPTIVE TECHNOLOGY

Some argue that humankind is on a path where it will no longer hold a monopoly on the conduct of war.¹⁰⁴ In many ways the change has been subtle. The same technology that has created slight changes in our day-to-day lives has enabled tremendous change on the battlefields of Iraq and Afghanistan.¹⁰⁵ Indeed, one cannot imagine the conduct of modern operations without the enabling capability resident in the unmanned drone. The integration of strong artificial intelligence into robot systems will cause a tremendous increase in capability, but it may not be recognized as a revolutionary event due to the proliferation of robots throughout the battlespace.¹⁰⁶ It is the transformation from systems that are tele-operated or very limited in their autonomous characteristics to systems that possess higher degrees of autonomy that has the potential to be disruptive. As long as robots remain tele-operated, they are no different than any other tool at a soldier's disposal. With strong AI, faster computers and more sophisticated mathematical algorithms on the horizon, robots have the potential to become more than mere tools.

102. "The United States Department of Defense maintains a Robotic Systems Pool (RSP) which consists of a ready inventory of robotic vehicles, payloads, and related components available on loan to requesting users in order to support research and development, experimentation, evaluation, training, and technology transfer. It provides users a low-risk quick-turnaround opportunity to gain access to new technologies that they might otherwise not see for years. The feedback attained from having operational subject matter experts evaluating technology at a relatively early stage can be invaluable. RSP also serves to facilitate technology adoption by overcoming some of the traditional barriers to user trials, again serving to bridge the gap between technology users and technology developers." See Nguyen et al., "Land, Sea, and Air," 9. The creation of a similar robotics pool in Canada would certainly contribute to technological socialization and the building of trust.

103. Hewitt, "Comments."

104. Singer, "Wired for War."

105. Deputy, *Counterinsurgency and Robots*, 1.

106. Deputy, *Counterinsurgency and Robots*, 5.

Autonomous robot systems could represent a true revolution in military affairs that has the potential to alter career fields, training pipelines, and combat tactics, techniques and procedures (TTPs). Army leadership need not fear the future, but must remain mindful of the need to skilfully manage the impact of this potentially disruptive technology.¹⁰⁷ The exact point in time at which autonomous systems will be ready for use in the battlespace is unknown, but the theory of disruptive innovation suggests that their arrival in that role is virtually certain.¹⁰⁸ It is highly unlikely that fully autonomous robot systems will be used in the Army of Tomorrow. Indeed, there are many technological limiters and institutional challenges which must be overcome before such systems have the potential to become reality. However, Horizon Three presents a realistic timeframe for the use of autonomous robot systems. These robots will be considerably less disruptive if their tele-operated and semi-autonomous counterparts continue to enter into service over the next two decades and experience ever-increasing degrees of success—and therefore acceptance.

4.8 NOTE ON PROCUREMENT

As with most Army acquisitions in the 21st century, there is omnipresent friction between capability developers and military procurement agencies. Because of the expense associated with defence procurement, acquisitions tend to take a long time; as a result, by the time a system is actually procured, its resident technologies may already be obsolete. The pace of procurement and the pace of technological change are not synchronized. Ideally, however, they would be. Such an expectation may be unrealistic for large and expensive systems, but it may be a more reasonable goal for less expensive systems. The maintenance of momentum and timely staff action are important components of speeding up the acquisition process. Jim Hewitt of the Directorate of Combat Systems Engineering Management describes EOD ROV procurement in support of Operation ATHENA:

High level direction and active support which is sustained for at least one full project cycle period (typically ten years) will also be needed. In the lifetime of EOD ROV Projects 0553 and 1111 [discussed earlier] the operational facts on the ground have changed swiftly, but initial

107. John Edward Jackson, "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform," *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136, 6.

108. Major D.A. Goldsmith, *Robots in the Battlespace: Moral and Ethical Considerations in the Use of Autonomous Mechanical Combatants*, Canadian Forces College JCSF 34. 29 July 2010: <http://www.CAFc.forces.gc.ca/papers/csc/csc34/exnh/goldsmith.pdf>, 17.

high level support rapidly declined, with a corresponding inability of both the requirements and procurement agencies to respond in a timely manner. It has taken almost three years to bring into operational service a small number of Dragon Runner™ sized ROVs procured under a UOR, and the timeline for the other ROV projects has passed the ten year mark. In sum, we are planning on delivering urgently required equipment after the war is scheduled to be over.¹⁰⁹

PART FIVE – LEGAL AND ETHICAL CHALLENGES

Tele-operated robot systems have seen use in the Army for over two decades, but larger, independently moving and operating UGVs have been much less prevalent. The mental images of an armed autonomous UGV firing at a perceived hostile target or of an unarmed autonomous UGV accidentally running over a civilian in the battlespace demonstrate the moral, legal, and ethical hurdles that confront Army leadership with respect to robot employment in an operational setting.¹¹⁰

Discussion regarding the legal and ethical challenges posed by robots is generally framed in terms of the Just War tradition. The idea behind that tradition is that war is objectionable yet unavoidable; the best that can be done is to place moral and legal constraints on entering into conflict and to then monitor the conduct of war itself with a view to discouraging war crimes.¹¹¹ It is important that international law clearly set the foundation for the acceptability of using robot systems across the continuum of operations. The following paragraphs ought not to be read as showstoppers in the further incorporation of robotics into the Army. Rather, they serve as paramount considerations in the employment of such systems once they are incorporated.

5.1 INTERNATIONAL LAW

Much like the procurement system, the laws of warfare struggle to keep pace with current technology.¹¹² Alternate means of modern warfare, such as cyber attack or the use of unmanned robotic systems, are not addressed in the United Nations Charter.¹¹³ There is probably already a need to revisit the

109. Hewitt, "Comments."

110. Nardi, *Autonomy*, 1.

111. Goldsmith, *Robots in the Battlespace*, 9.

112. McDaniel, *Robot Wars*, 10.

113. McDaniel, *Robot Wars*, 10.

existing provisions in international law, the law of conflict, and agreements such as the Geneva Convention.¹¹⁴ The present use of robots in military operations already raises significant legal issues, especially in terms of armed robots like SWORDS or Predator. Partly because the legal rationale behind the use of these armed systems has not been declared, the international community is becoming increasingly convinced that the use of robot systems constitutes a violation of international law.¹¹⁵ Some pundits believe that the Ottawa Convention itself may provide sufficient guidelines to block any future development of armed robotic systems despite their increasing ability to discriminate.¹¹⁶

The laws of warfare will allow unmanned robotic systems to operate as human extensions in the contemporary operating environment (i.e., tools). However, as unmanned robotic systems become more technologically complex, laws that govern the design and production of these systems will likely become more stringent.¹¹⁷ Consideration must also be given to determining who is a lawful combatant. Is the Air Force pilot flying a Predator from thousands of miles away in Nevada, or the civilian contractor servicing it in on an airstrip in Afghanistan, a lawful combatant?¹¹⁸

5.2 RESPONSIBILITY

Who is at fault if something goes wrong?¹¹⁹ Blame could be placed on (or shared among) the commander, the operator, the programmer, the victims, or perhaps the machine itself.¹²⁰ The answer to this question is not straightforward even today, despite the fact that the overwhelming majority of military robotics are tele-operated. As technology enables militaries to allow robots increasing degrees of autonomy, this question will become much more difficult to answer.

To put things in perspective, we must consider the degree in which AI already plays a role in military decision making. The fighter pilot relies crucially on targeting information provided by AI when deciding whether or not to destroy a target. If this information turns out to be wrong—perhaps even deliberately

114. Dewar Donnithorne-Tait, "Unmanned Systems: A Defence Perspective," *Frontline Defence* (Sept/Oct 2009): 24. 29 July 2010. http://www.alberta-canada.com/documents/AIS-AERO_UnmannedSystems-DefencePerspective.pdf.

115. Anderson, "Testimony," 1.

116. Hew, *The Generation*, 10.

117. McDaniel, *Robot Wars*, 76.

118. Tierney, "Testimony."

119. McDaniel, *Robot Wars*, 16.

120. McDaniel, *Robot Wars*, 52.

misleading—can we still hold the pilot responsible?¹²¹ If we cannot, then who holds the responsibility? A pilot will make the decision to engage if the onboard AI indicates that something is a legitimate military target. One might argue that this is simply an illusion of human decision making. In that respect, it would not be such a big leap of faith to take that human pilot out of the loop all together.

It must also be noted that smart technologies that allow robot systems to learn from their experiences (or the experiences of other systems) must by default obliterate claims of responsibility by system programmers. “The possibility that an autonomous system will make choices other than those predicted and encouraged by its programmers is inherent in the claim that it is autonomous. If it has sufficient autonomy that it learns from its experience and surroundings then it may make decisions which reflect these as much, or more than, its initial programming.”¹²² In a similar vein, operators or system managers cannot be held to account when machines are given the ability to learn. Experts concur that there is tremendous difficulty in ascribing responsibility to an operator of a machine that employs learning algorithms, since in principle the operator is no longer capable of predicting the machine’s future behaviour.¹²³

Assigning responsibility to computer programmers is not feasible. Although some proponents argue that licensing would strongly encourage professionals working in the computer industry to follow the highest standards of their industry, and that licensing would allow violators to be legally investigated, it is not reasonable to expect them to conceptualize all the complexities of an actual conflict zone.¹²⁴ Other factors, such as the number of individuals assisting in the creation of the robot’s software, may preclude the notion of programming accountability.¹²⁵ Many individuals who work in the field of information technology are specialized technicians trained to perform highly detailed tasks that are very compartmentalized in nature. Their jobs do not require them to visualize the overall purpose of the system under programming and assembly, but simply require them to make the system functional.¹²⁶

121. Sparrow, “Killer Robots,” 69.

122. Sparrow, “Killer Robots,” 70.

123. Arkin et al., *Responsibility and Lethality*, 3.

124. McDaniel, *Robot Wars*, 69.

125. McDaniel, *Robot Wars*, 28.

126. McDaniel, *Robot Wars*, 65.

However, some argue that ethical decision making by a machine is only as good as the human who programs it and the state of technology that exists at the time. Therefore the humans behind the technology are indeed ethically liable.¹²⁷ However, ethical programming may be as simple as building in the requirement for human authorization at different stages in the robotic decision-making process. In effect, the issuance of a command override changes the status of the machine from that of an autonomous robot to that of a robot serving as an extension of the soldier, and operator(s) who used the override would accept all responsibility for their actions.¹²⁸

It is the prospect of intelligent actors without any moral responsibility that makes ascribing legal responsibility challenging and which makes robotic warfighters especially terrifying. Here, an analogy may be drawn with child soldiers. When child armies take to the battlefield, as they have in Angola and Liberia in recent years, no one is in control. If civilians are killed, they are killed senselessly without anyone being responsible for their deaths. In a sense, deaths occur indiscriminately—without necessarily being random. There seems to be a conceptual space in which children and perhaps machines are sufficiently autonomous to make the attribution of responsibility to an appropriate adult problematic, but not so autonomous as to be responsible for their own actions.¹²⁹ Before Canada deploys robot systems that are employed under the auspices of the Act operational function, this gap must be recognized, communicated, and resolved, or else significant risk must be accepted.

To be permissible, war must be the last resort available to a state intending to pursue a just cause, and circumstances must indicate a reasonable chance of succeeding in a proportionate manner. Once the state is at war, harms must be necessary and proportionate.¹³⁰ These are the two principles of “just war,” known universally as *jus ad bellum* and *jus in bello* respectively.

5.3 JUS AD BELLUM

The paradox yet to be resolved under the principle of *jus ad bellum* is that robot systems will ensure that war is ended more quickly and efficiently while

127. McDaniel, *Robot Wars*, 20.

128. Arkin et al., *Responsibility and Lethality*, 4.

129. This analogy is borrowed from Sparrow, “Killer Robots,” 74.

130. Dr. Edward Barrett, “Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform,” *Rise of the Drones: Unmanned Systems and the Future of War*, 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136.

ensuring that fewer lives are lost in its conduct; however, because of this, robots will also make the very decision to go to war more likely.

Cost reductions, including those afforded by unmanned systems, allow states to more readily pursue just causes, but favourable alterations to pre-war proportionality calculations could also reduce the rigour with which non-violent alternatives are pursued.¹³¹ The ability to make the decision to go to war easier presents potential changes in the law of war principle of proportionality: since war is easier, at least for those nations with advanced technologies, there may be more wars.¹³² Moreover, removing humans from armed conflict further disconnects humans from war, thus making it easier to physically wage war.¹³³

Some believe that robot systems will ultimately change society and condition humans to become more desensitized to the violence of war.¹³⁴

When a citizenry has no sense of sacrifice or even the prospect of sacrifice, the decision to go to war becomes just like any other policy decision, weighed by the same calculus used to determine whether to raise bridge tolls. Instead of widespread engagement and debate over the most important decision a government can make, you get popular indifference ... without public debate and support and without risking troops; the decision to go to war becomes the act of a nation that doesn't give a damn.¹³⁵

Removing the threat of death to people for only one side of a war creates a situation that is potentially as morally asymmetric as it is physically.¹³⁶

Other unresolved questions here include: (1) would it be an act of aggression to deploy a robot into another sovereign country's territory?¹³⁷ and (2) if you could invade other countries bloodlessly, would this lead to a greater temptation to invade?¹³⁸

131. Ibid.

132. McDaniel, *Robot Wars*, 11.

133. McDaniel, *Robot Wars*, 4.

134. McDaniel, *Robot Wars*, 30.

135. Quoted from Singer, "Robots at War."

136. Goldsmith, *Robots in the Battlespace*, 5.

137. Fielding, "Robotics," 106.

138. Crispin, "What Killed."

The Geneva Convention provides several useful principles to consider in understanding the philosophy of *jus in bello*: (1) Attackers must be capable of distinguishing the civilian population from combatants. Neither the civilian population as a whole nor individual civilians will be attacked. (2) Attacks are to be made solely on military targets. Individuals who can no longer take part in hostilities are entitled to respect from their attackers. (3) It is strictly forbidden to kill or wound an adversary who surrenders. (4) Weapons or methods of warfare that inflict unnecessary suffering or destruction are forbidden. (5) Wounded combatants and sick combatants must be cared for as soon as possible. (6) Combatants must be able to distinguish the universal Red Cross or Red Crescent on a white background. All combatants are forbidden to engage objects thus marked. (7) Captured combatants and civilians must be protected against all acts of violence.¹³⁹ For robotic systems operating autonomously, the inability to distinguish the difference between a lawful and unlawful target remains the overall issue while operating within the confines of the law of war. Unmanned robotic systems must remain under the control of human operators until the issues of discrimination and proportionality can be resolved.¹⁴⁰

A necessary condition for fighting a just war, under the principle of *jus in bello*, is that someone can be justly held responsible for deaths that occur in the course of the war. As this condition cannot be met in relation to deaths caused by an autonomous weapon system, it would therefore be unethical to deploy such systems in warfare.¹⁴¹ Using this logic, one could similarly argue that employment of the Aegis system is a violation of the Law of Armed Conflict. Therefore, as of today, in order to abide by this convention, robots must remain under tele-operated or semi-autonomous control at all times when the person controlling the robot makes the ultimate decision to fire.¹⁴² This consideration alone is enough to suggest that the prospects for fully autonomous machines are more remote than is sometimes claimed.¹⁴³

It should also be noted that there are ethical dilemmas in the conduct of war pertinent to tele-operation as well. Soldiers engaged in such virtual warfare

139. McDaniel, *Robot Wars*, 13.

140. McDaniel, *Robot Wars*, iv.

141. Sparrow, "Killer Robots," 62.

142. McDaniel, *Robot Wars*, 15.

143. Sparrow, "Killer Robots," 66.

are less situationally aware (an argument put forward by pilots advocating for the continued use of manned fighter aircraft), and also less restrained because they are more emotionally detached.¹⁴⁴ Although the standoff afforded the human operator is certain to lessen the likelihood that a target will be engaged for emotional reasons, that standoff may well serve to dehumanize the target, potentially creating a situation where the decision to engage is made with the same level of rigorous thought used in the conduct of a first-person-shooter video game.

The leading contrarian to these views is Ronald Arkin, who argues that although responsibility for the use of unmanned systems must be made clear, it is not infeasible to do so.¹⁴⁵ He argues that as long as responsibility for robot behaviour is unambiguous and clearly attributable to a particular human, then the ethical dilemmas associated with these systems are easily resolved. Others argue that the very ability to construct robots to operate in a perfectly moral manner (thus perfecting *jus in bello*) would constitute a violation of *jus ad bellum* due to the overwhelming overmatch given to the side that is armed with robots.¹⁴⁶ That said, nothing precludes their use in roles that reduce the risk to our soldiers but do not involve killing the enemy.¹⁴⁷

Ironically, robots of today have already broken Isaac Asimov's First Law of Robotics: "a robot may not injure a human being."¹⁴⁸ In fact, the very act of building lethal combat robots means that humans have already violated the intent of all of Asimov's robot laws.

5.5 ETHICS

There are two ethical arguments concerning the use of robot systems in the conduct of warfare. One side argues that every advantage should be seized in war as long as it leads to victory with as few people harmed as possible. The other argues that such a move would be morally repugnant because it assigns asymmetric value to the human lives of the soldiers on the two sides of the conflict.¹⁴⁹

144. Barrett, "Testimony."

145. Arkin et al., *Responsibility and Lethality*, 1.

146. Goldsmith, *Robots in the Battlespace*, 17.

147. Goldsmith, *Robots in the Battlespace*, 17.

148. McDaniel, *Robot Wars*, 79.

149. Goldsmith, *Robots in the Battlespace*, 11.

The key question is whether or not these systems perform better at ethical decision making than do human soldiers. In response, the following may be contended:

- Robot systems possess the ability to act conservatively. They do not need to protect themselves in cases of uncertainty or poor target identification.
- Advances in technology will allow unmanned systems to be equipped with better sensors than human soldiers currently possess.
- Robot systems do not possess emotions such as anger that cloud judgment.
- Robot systems can process more information from a vast number of sources more quickly and accurately than can human soldiers before responding with lethal force.
- Robot combat systems are capable of accurately reporting during stressful combat situations without emotional exaggeration, distortion, or contradiction.
- While working with human soldiers, they can objectively monitor ethical behaviour on the battlefield and report any ethical violations that might be observed.¹⁵⁰

Sensor improvements, lack of fear-induced haste, reduced anger levels, and crystal clarity about strike damage all combine to actually enhance awareness and restraint. If true, it may be unethical not to use robot systems.¹⁵¹ Put another way, we may be obligated to use robots because they will save soldiers' lives.¹⁵² Moreover, effectiveness and efficiency are fundamentally moral imperatives. Constituted and supported by its citizen taxpayers, the liberal democratic state is morally obligated to effectively defend their human rights with their limited resources.¹⁵³

150. McDaniel, *Robot Wars*, 16–17.

151. Barrett, "Testimony."

152. Goldsmith, *Robots in the Battlespace*, 11.

153. Barrett, "Testimony."

5.6 LIABILITY

Beyond the obvious issues related to lethal engagement, consideration must also be given to unintentional consequences of employing robot systems. For example, the mixture of human-operated vehicles and unmanned vehicles sharing the same roads will become extremely difficult to manage.¹⁵⁴ The inherent liability issues must be studied in depth before the use of unmanned robot systems increases in future conflict.¹⁵⁵ As a modern-day example, the Global Hawk lands and takes off in a fully autonomous mode. If the operator is unable to see an unsuspected obstacle on the airstrip—such as a car, another aircraft, or children playing ball—there may be disastrous consequences before the operator can override the Global Hawk’s landing function.¹⁵⁶ Issues of liability must be well thought out, ideally prior to their resolution in an international court. That may be as simple as adopting the approach currently used to compensate local populations for collateral damage they suffer as a result of military operations. Of course, another thing to consider is the psychological impact that the employment of robots could have on local populations. Is emotional trauma something for which a force should be held liable?

PART SIX – IMPACT ON THE OPERATIONAL FUNCTIONS

Robots represent the potential for significant impact across the five operational functions. The greatest possibilities for success in the near future lie in the Sense and Shield domains, but robots also have the ability to significantly affect the Command and Sustain functions within the Army of Tomorrow. Though impact, on the Act function will initially be limited in the Future Army, that function will also undoubtedly be shaped by the employment of unmanned systems.

6.1 COMMAND

The operational function of Command is affected in three ways: communications, battlespace management, and human control. Impacts related to leadership and related intangibles are discussed in detail in the PRICIE analysis below.

154. McDaniel, *Robot Wars*, 15.

155. McDaniel, *Robot Wars*, 15.

156. McDaniel, *Robot Wars*, 47.

Robot systems can be used as platforms by command support elements. For example, robots can be employed as communication re-transmission or re-broadcasting nodes that position and reposition as the force moves, in order to optimize connectivity. All robotic systems will have the ability to communicate and can therefore act as relay nodes for command and control (C2) communications.¹⁵⁷ Another role for robotics lies in the reduction of deliberate electromagnetic emission signatures through distancing or dispersion.¹⁵⁸ Rather than developing separate command support platforms, it is more likely that such capabilities would be piggybacked onto other robotic platforms.

The use of robotic systems with autonomy (or limited autonomy) will inevitably increase the pace of war, given that robots will be able to move, gather information, conduct analysis, make decisions and execute tasks more rapidly than their human counterparts. That will impose new management responsibilities on operators managing teams of unmanned ground and aerial systems and introduce new management challenges for commanders.¹⁵⁹ The issue will be trust: commanders will have to decide whether or not to put their faith in robotic analysis and decision making. Additionally, robot systems must know when and how to communicate.¹⁶⁰ In other words, robots will need to report their location and intended movements, at tempos demanded by battlespace management systems. This may compromise robot freedom of movement and will add to communication loads.¹⁶¹

Should armed robotic systems ever make up a part of the Army, there will be additional strains placed on humans conducting battle management functions. Armed weapons on the battlefield—whether tele-operated, fully autonomous or something in between—changes the character of the battle management process in the following ways:

- The number of weapons under the control of a single operator is increased greatly.
- The rate at which weapons can be launched is increased greatly, limited only by the rate at which the targets appear, rather than by the rate at which a human operator can handle them.

157. DoD, *Roadmap 2009–2034*, 14.

158. Fielding, "Robotics," 102.

159. McDaniel, *Robot Wars*, 60.

160. Trentini et al., *Autonomous Land Systems*, 14.

161. Hew, *The Generation*, 7.

- The rate at which decisions must be made is increased greatly, driven by the number of weapons available and the rate at which they are launched.
- If an operator must make or approve all launch decisions, the launch rate will be constrained by the operator's decision and reaction time.¹⁶²

It should be noted that battle management concerns primarily relate to the employment of systems with degrees of autonomy beyond tele-operation, as tele-operated systems are normally governed by the rule of one operator per platform.

The ability or inability of an unmanned or robotic system to correctly decide when, where, and how to apply force in keeping with the operational and strategic objectives must be considered.¹⁶³ The general vision for manoeuvrable unmanned systems is that they will operate autonomously and be managed as a group by a single operator, the same way a flight controller manages the aircraft in the airspace around a commercial airport.¹⁶⁴ The implication is that the operator of multiple systems needs to be viewed as a system manager, managing multiple subsystems and monitoring their decisions and actions, and approving plans rather than making detailed decisions.¹⁶⁵

6.2 SENSE

The Army publication *Future Force* discussed at length how robots will fit into the ISTAR system:

Sense capabilities will make maximum use of robotics and autonomous intelligent systems. Unmanned aerial and ground vehicles equipped with multi and hyper-spectral sensors will add redundancy, range and accuracy to future reconnaissance and surveillance capability, while reducing the risk to the soldier of having to physically collect the information (i.e., eyes on the target). In time, the requirement for human involvement in traditional reconnaissance and surveillance activities will be reduced in favour of unmanned or unattended sensors. With the possible exception of human intelligence (HUMINT), soldiers in the future will be

162. Hanon, *Robots on the Battlefield*, 7.

163. Deputy, *Counterinsurgency and Robots*, 11.

164. Hanon, *Robots on the Battlefield*, 6 and 9.

165. Hanon, *Robots on the Battlefield*, 7.

employed less and less in the physical task of collecting data, and increasingly in the mental task of analyzing and interpreting the data that is amassed.¹⁶⁶



The potential for robots to be high-value contributors to the overall ISTAR system is already recognized.¹⁶⁷ There are two types of considerations with respect to the operational function of Sense: (1) system sensors and (2) “system as sensor.” System sensors are discussed at length in the PRICIE analysis below.

The linkage between the operational functions of Command and Sense is usually expressed in terms of C4ISR. The optimal C4ISR system delivers relevant information to commanders and staff rather than simply being a high-tech paralysis-inducing information colossus. It is therefore not enough to say that we need more ISTAR capability. We must define more precisely the

166. Quoted from *Future Force*, 112.

167. Hew, *The Generation*, 8.

information we need and then determine the optimal mix of sensors that can deliver that information. The Army does not need more ISR systems, it needs better C4ISR systems.



Army tactical commanders want to know what is immediately beyond their line of sight and what targets are within range of direct and indirect fire weapons. Analysis of sensor products, typically optical or infrared imaging, is often difficult due to ground clutter.¹⁶⁸ Unmanned systems offer unique sensing capabilities in that they make no distinction between line of sight and beyond line of sight.¹⁶⁹ Simply piling on more aerial-based sensors may not be the best answer. However, both air- and ground-based robots that have the ability to enter structures in order to gain information have the potential to greatly enhance the ISTAR system. UAVs have been recognized as high performers in the role of remote reconnaissance and surveillance, and there is great future utility for reconnaissance UGVs, particularly in confined,

168. Donnithorne-Tait, "Unmanned Systems," 20.

169. Hew, *The Generation*, 5.

complex, and hazardous environments.¹⁷⁰ It should be noted that these are precisely the environments that pose problems for today's generation of UGVs. In other words, they have difficulty understanding such environments.

Developing UGVs with enhanced functionality that specifically supports persistent surveillance and reconnaissance applications is essential. New operational capabilities derived from this effort will include the ability to conduct continuous covert unmanned surveillance from a remote location (analogous to a human-occupied observation or listening post).¹⁷¹ Tunnel, sewer, cave, and urban structure reconnaissance are also potential tasks.¹⁷²

Robots can also play a role in shortening the targeting process, enhancing the detection, recognition, identification, location, and marking of targets. They could also be used in the mounting of decoy high-value targets to unmask enemy weapon systems for targeting by other systems.¹⁷³ The most practical role outlining an unmanned robotic system's position in war is the collection of detailed intelligence that will be exploited against the adversary. As a result, one may think of this process as the groundwork for precision targeting.¹⁷⁴ For UGVs equipped with or having access to weapons or linked to weapons effects, tactical behaviours must include targeting, engaging, and assessing damage.¹⁷⁵

Robots could be effectively employed to acquire geospatial data and to position differential GPS stations.¹⁷⁶ When aerial surveillance is not available, ground-based robots can be used to survey IED hotspots for extended periods of time.¹⁷⁷

The Army does not need UAVs to see around corners. The capabilities that currently exist in the Air Force can do that. In a multinational context, Predators and Reapers are providing more than 700 hours of full-motion video every day (more than 22,000 hours per month) to coalition ground forces in both Iraq and Afghanistan, providing unmatched persistence and flexibility.¹⁷⁸ Every second of every day, forty Predator-series aircraft are

170. Fielding, "Robotics," 103.
171. Nguyen, et al., "Land, Sea, and Air," 5.
172. Nguyen, et al., "Land, Sea, and Air," 1.
173. Fielding, "Robotics," 104.
174. McDaniel, *Robot Wars*, 31.
175. Trentini et al., *Autonomous Land Systems*, 14.
176. Fielding, "Robotics," 105.
177. Chris Lefkow, *US Army Lt Gen Wants Unmanned Ground Vehicles*, Agence France-Presse, 12 August 2009, 29 July 2010: <http://www.defensenews.com/story.php?i=4231507>.
178. Michael S. Fagan, "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform," *Rise of the Drones: Unmanned Systems and the Future of War*, 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136, 7.

airborne worldwide.¹⁷⁹ However, smaller UAVs that have the ability to hover or even fly inside structures have the potential to close the gap in urban reconnaissance and terrain mapping that presently exists. These UAVs can fill a critical need, providing actionable intelligence and decreasing the time between sensor and shooter, thus shortening the kill chain.¹⁸⁰ Not to say that such robots need to fly. A UGV that fills the same gap would be equally desirable.

6.3 ACT

Act is the operational function that integrates firepower, manoeuvre, and offensive information operations to achieve desired effects. It is important to consider the Act function carefully and not simply marginalize it based on unfounded fears of the weaponization of autonomous robotic systems (and the attendant concerns about legalities, ethics, and morality). Concerns about lethality need not hamper developments in the area of autonomy. That said, it is important to note that there is a key delineation between military applications of unmanned systems, that is, there are those that are designed to kill the enemy and those that are not.¹⁸¹ The Act function goes beyond the simple killing of the enemy, though this particular application in and of itself must be considered as well.

Robot systems offer the ability to engage with small arms fire more accurately than human soldiers due to increased platform stability and the ability to better absorb recoil. SWORDS was able to hit the bull's eye of a target at 2,000 metres and could hit a nickel-sized target 70 out of 70 times at 328 yards.¹⁸² Robots could be sent on high-risk or suicide missions that would not have been considered before.¹⁸³ Not all kinetic effects are necessarily lethal. The MDARS sentry robot uses FN303 paintball guns queued by the on-board personnel-detection radar to achieve its effect.¹⁸⁴

Robots can be weaponized to conduct tasks ranging from non-lethal to lethal, in a crowd control role or in the conduct of combat operations.¹⁸⁵ An unmanned vehicle could also be used as an armed wingman—a fighting

179. Fagan, "Testimony," 7.

180. Fagan, "Testimony," 8.

181. Fielding, "Robotics," 101.

182. Cowan, *Theoretical, Legal and Ethical*, 7.

183. Cowan, *Theoretical, Legal and Ethical*, 3.

184. Nguyen, et al., "Land, Sea, and Air," 7.

185. DoD, *Roadmap 2009–2034*, 10.

platform which mirrors the actions of a manned vehicle.¹⁸⁶ Unmanned vehicles can also be employed in support of psychological operations and in support of electronic warfare and navigation warfare.¹⁸⁷ All of these types of robotic applications are constrained by standing and mission-specific rules of engagement requirements which will need to be thought through before any systems can be employed as part of the Act function.

The US military will eventually allow unmanned robotic systems to autonomously employ lethal force.¹⁸⁸ Weapon systems such as the Patriot Air Defence Weapon System, the Aegis Automatic Special Weapon System, and the Tomahawk Anti-Ship Missile System are current examples of automated systems (note that they are not considered robots) capable of lethal effects with little or no human intervention.¹⁸⁹ The development of autonomous lethal robotic systems is well underway and it may be simply a matter of time before targets can be engaged autonomously on the American battlefield.¹⁹⁰ Autonomy and moral responsibility go hand in hand. To say that agents are autonomous is to say that their actions originate in them and reflect their ends. As already discussed, Army capability developers must be mindful of the fact that where a robot acts autonomously, it is not currently clear who is responsible for its actions.¹⁹¹

At present, systems capable of performing in the Act domain include tele-operated robots and unattended systems akin to landmines. Australian defense analyst Patrick Hew provides clarification:

Consider the notional assemblage of an acoustic sensor being monitored by a human being, who in turn operates a rifle on remote control. If the human being is working purely from the sensor data, then it is effectively beyond-visual-range combat and the authorization for the human to fire is the familiar issue of mission command, and rules of engagement in particular. Now remove the human link between sensor and shooter, and replace it with a direct (electronic) link. That is, the acoustic sensor report is the shooting cue for the rifle. Such a system is functionally equivalent to a land mine, merely more aware. The challenge to conceptual systems like

186. Lefkow, *Gen Wants Unmanned Ground Vehicles*.

187. Fielding, "Robotics," 103.

188. McDaniel, *Robot Wars*, 20.

189. McDaniel, *Robot Wars*, 35.

190. Arkin et al., *Responsibility and Lethality*, 1.

191. Sparrow, "Killer Robots," 65.

these is, therefore, in their capacity to discriminate—not in their capacity for automated action.¹⁹²

Thinking of robots as smart mines, however, will hinder their acceptance into the Act function. It also raises concerns about how robots fit into the national interest, as explicitly laid down in the Ottawa Convention. The US has already embraced the idea of employing unmanned systems within the Act function:

The challenge here is to embrace the concept of armed autonomy wholeheartedly and to set system design requirements that fully exploit what these systems can do. There is a danger here that legacy remote control system experience will lead the system requirements to be set well below what is possible. This would limit severely the performance and value of these new systems without reducing their cost. Development of new technical systems is by its nature goal driven. Demanding less of these armed autonomous systems than is possible will compromise and jeopardize both their development and their value in the field. If these goals are set too low the resulting systems will be seen as expensive versions of systems already fielded, rather than the quantum leap in war fighting technology that they can be.¹⁹³

Before the use of robots for the generation of lethal effects can be considered, a climate of trust between robots and soldiers must be established. Once that is in place, the question can be revisited. For now, the consensus appears to be that robots should not be allowed to kill humans unless a human being is in the loop, which seems to point toward a future of “video game warfare” with a tele-robotic motif.¹⁹⁴

On a final note, the diffusion of robots on the battlefield may result in more robust attempts by belligerent forces to conceal themselves. An enemy that would unmask to destroy a human adversary would likely not be so quick to unmask to destroy an unmanned system. Such considerations may drive design requirements for robot systems that are indistinguishable from their manned counterparts.

192. Hew, *The Generation*, 5.

193. Hanon, *Robots on the Battlefield*, 10.

194. Lance Winslow, *Unmanned Vehicle Robotic Warfare: Hide and Seek Strategies*. Online Think Tank 18 May 2007. 29 July 2010: <http://www.worldthinktank.net/pdfs/unmannedvehiclerobotic.pdf>, 11.

6.4 SHIELD

Unmanned robotic systems replacing humans in acts of conflict conveniently suits the Western nations' intolerance of casualties.¹⁹⁵ The conduct of tasks that are dirty, such as CBRN defence, and dangerous, such as EOD, represents the ability to truly shield the human force. Potential tasks for robots within the Shield function largely centre on combat engineering. They include the clearance of land-mines, booby-traps, mines and unexploded explosive ordnance (UXO) through spoofing or by detection and neutralization; detection, identification and marking of areas contaminated with CBRN and other hazardous materials; positioning of demolition charges for the demolition of buildings and bunkers with mass blast effects; the construction of complex obstacles including the laying of minefields and digging of anti-tank ditches; and general survivability support, particularly in the mounting of decoy vehicles, equipment and multi-spectral smoke generators in accordance with a deception plan.¹⁹⁶ There are essentially two items that must be considered under the Shield operational function: (1) Shield the Robot; and (2) Shield the Force.

6.4.1 SHIELD THE ROBOT

Survivability must be a design consideration of any robot system. Relevant survivability techniques include the robot's ability to change battle positions, dash from one point to another, hide and call for additional support.¹⁹⁷ If captured, a UGV might not hesitate to call in artillery on itself or simply self-destruct, so long as certain conditions are met first.¹⁹⁸ Of particular concern for armed robots or robots that transport weapons and munitions is the possibility of enemy capture. Safeguards must be in place that will prevent unauthorized persons from gaining control of these robotic systems.¹⁹⁹ These safeguards ought not to include lethal measures. In other words, the killing of human beings should never be required simply to preserve a robot. Unmanned systems must value civilian lives above their own.²⁰⁰

For robots to be effective they must be engineered to reduce vulnerabilities to electronic and navigation warfare and to provide protection against the

195. McDaniel, *Robot Wars*, 4.

196. Fielding, "Robotics," 104.

197. Trentini et al., *Autonomous Land Systems*, 15.

198. Trentini et al., *Autonomous Land Systems*, 15.

199. Department of the Army, *Robotics Strategy White Paper*, 21.

200. Arkin et al., *Responsibility and Lethality*, 1.

capture of any secure communications equipment carried by the robot. The robot must also be able to inform human controllers when it has been physically compromised.²⁰¹ A greater measure of survivability is desirable in order to protect the investment, but it also must be balanced against degradation in range and payload capabilities.²⁰² Since a few large, sophisticated platforms would be exceedingly expensive, perhaps it would be wiser to invest in many small, simple systems that are able to cooperate and collaborate, so that losing a few systems would not represent a significant loss of investment. Moreover, the capture of a few simple systems by the enemy would not provide them with much capability, since it would take many such systems to achieve significant capability levels.

6.4.2 SHIELD THE FORCE

Environments contaminated with toxins such as chemicals, biohazards, and radiation will not affect a machine's judgment or its ability to execute tasks.²⁰³ Therefore, robots can be used to detect and identify hazards and to communicate that information to the human first responders located at a safe distance from the hazard. They could also play a role in containing the toxin or reducing its spread, or in handling, clean-up, transport, and general management, including disposal or destruction, of the hazard.²⁰⁴

Clearance of mines, booby-traps, and other obstacles ahead of friendly movement is a valuable application for robotics.²⁰⁵ Indeed, it makes sense to incorporate robotic unmanned systems to locate, detonate, or de-activate roadside bombs using sensors, tele-robotics, and sniffers.²⁰⁶ Remotely operated systems can provide excellent solutions in a variety of hazardous operations such as counter-mine and counter-IED. For those applications, tele-operated systems may be the best option for the foreseeable future.²⁰⁷ However, it should be noted that there is a great deal of research on counter-IED systems, therefore they are likely to become much more automated in the future.²⁰⁸

Robots can also be used for tasks beyond mine clearance and the neutralization of more sophisticated explosive ordnance. Such tasks include fire fighting,

201. Fielding, "Robotics," 106.

202. DoD, *Roadmap 2009–2034*, 29.

203. McDaniel, *Robot Wars*, 37.

204. Stocker, *Autonomous Intelligent Systems*.

205. Fielding, "Robotics," 102.

206. Winslow, *Unmanned Vehicle Robotic Warfare*, 31.

207. Donnithorne-Tait, "Unmanned Systems," 19.

208. Donnithorne-Tait, "Unmanned Systems," 21.

decontamination, forward operating base security, installation security, obstacle construction and breaching, and vehicle and personnel search and inspection.²⁰⁹

Robots could also be used to mount decoy vehicles and equipment which move in accordance with a deception plan.²¹⁰ In this respect, an engagement skill for a robotic system could include the ability to draw lethal fire away from accompanying manned platforms.²¹¹ The unmasking of enemy capabilities would allow their destruction by manned and unmanned systems alike, as already discussed in the previous section.

6.5 SUSTAIN

Given that the commercial and industrial worlds have experienced automation through the use of robotics for several decades now, it is no surprise that the tasks most readily suited to execution by robots are those within the logistics realm. Potential applications of robotic systems within the Sustain operational function include supply and resupply tasks, medical tasks, and repair and recovery tasks.

Resupply: follower mules for the carriage of stores, weapons and other equipment behind mounted or dismounted elements; Supply: robots may also be utilised as labour-saving devices in the handling of inventories and the packaging of supplies such as bulk water; Medical: robots could potentially be used to evacuate casualties from forward battle areas to medical facilities. The use of robotics in remote diagnosis and surgery is currently well established in advanced medical centres in the Western world; and Recovery and Repair: robots could be used to populate equipment repair facilities and to recover vehicles and equipment, particularly from combat zones.²¹²

Transportation of supplies will be a common task. Maintenance-type tasks such as inspection, decontamination, and refuelling could also be performed by unmanned robotic systems. Munitions and material handling and sustainment engineering are ideal tasks that could be allocated to robots to increase safety and increase efficiency.

209. DoD, *Roadmap 2009–2034*, 11.

210. Fielding, "Robotics," 103.

211. Trentini et al., *Autonomous Land Systems*, 14.

212. Quoted from Fielding, "Robotics," 105.

Casualty evacuation and care, human remains evacuation, and urban rescue are also potential tasks which could be performed by unmanned systems.²¹³ Other tasks include medical resupply, telemedicine, casualty care, and trauma stabilization. Because of the lack of human presence, manoeuvrable unmanned systems are precisely the ideal solution for nuclear and bio-weapon forensics and for contaminated remains recovery.²¹⁴

6.5.1 TACTICAL LOGISTICS SUPPORT

Under the concept of ADO, units are widely dispersed across a large theatre of operations but are linked through C2 systems that permit rapid, flexible application of supporting fires and coordinated employment of dispersed forces. Although units are more widely dispersed in ADO, the concept envisions a reduced logistics structure and small forward footprint through reach-back and distribution-based sustainment. Robotics technologies and UAVs could reduce the number of convoys required to support a large number of small units widely separated by unsecured lines of communication (LOCs), reduce soldier exposure along LOCs, and free up personnel, vehicles, and equipment for those convoys that are still necessary.²¹⁵

Convoys with manned lead vehicles and slave robotic followers are close to a reality²¹⁶ and should be fully functional within Horizon Two. Such technology can be employed to cut down both the number of combat service support vehicle operators and the risks they face.²¹⁷ The adoption of semi-autonomous vehicles within logistical convoys should be integrated only once the supporting technologies are truly ready.

6.5.2 OPERATIONAL AND DOMESTIC SUPPORT

Beyond tactical considerations, robotics can have applications pertinent to logistical rear operations. The US military is currently developing ground robots that can do useful work safely alongside humans in existing military facilities—the large warehouses where supply support activities take place.²¹⁸ Robots can use radio frequency identification (RFID) tags to inventory assets,

213. Quoted from DoD, *Roadmap 2009–2034*, 12.

214. Quoted from DoD, *Roadmap 2009–2034*, 14.

215. Department of the Army, *Robotics Strategy White Paper*, 10.

216. Donnithorne-Tait, "Unmanned Systems," 20–21.

217. Lefkow, *Gen Wants Unmanned Ground Vehicles*.

218. Tanya L. Trebes, "Agile Robotics," *Army* (March 2010): 100.

avoid storing incompatible items together, and select stock based on prevailing business rules and product attributes such as shelf life.²¹⁹

Current American logistics R&D effort is focused on accurate pallet detection and localization; stable, efficient operation over uneven terrain; detection of nearby pedestrians, obstacles and vehicles; natural speech and gesture interfaces; RFID integration; and detection of shouted warnings. There is also focus on the development of improved manipulation capabilities (pallet stacking / subpallet manipulation), and recognition and execution of more abstract, higher-level voice commands. Other potential enhancements include operation in more adverse environments (dust, rain, snow, night, GPS-denied areas); multitask optimization (more robots, fewer operators/supervisors); integration with back-end automatic identification system / decision-support environments; improved sensor fusion and human / machine interface, including understanding of ground-guide hand signals and spoken directions; and improvements to the robotic vehicle form, fit and function.²²⁰

The idea of automating the rear echelons may not, at first, seem to be the most useful robotic application. However, automating the rear means that fewer human resources are required. This in turn could free up soldiers to fill the ranks in the fighting echelon.

6.6 TASK ANALYSIS

A rudimentary analysis of the older DGLCD Task Lists, which contain more than 200 common Army tasks categorized by associated operational function, reveals some remarkable numbers.²²¹ The Table at Figure 2.6.1 suggests that more than one-third of the Army's tasks have the potential to be performed by, or with the assistance of, robots. Most of the tasks unsuitable for robots lie in the cognitive plane, where tasks consist mainly of analysis and planning.

An in-depth analysis of the DGLCD Task List may reveal more precisely areas well suited to robot application. Such an analysis could be backed up through more rigorous operational research supported by simulation.

219. Trebes, "Agile Robotics," 102.

220. Quoted from Trebes, "Agile Robotics," 104.

221. The DGLCD Task List is described in detail in the Annex at the end of this study.

The Table at Figure 2.6.1 shows that many of the tasks unsuitable for robots will eventually be well suited to AI resident on static computing networks, but detailed consideration of that fact is beyond the scope of this particular study. There are few tasks within the Command function suited to robots (other than physical tasks such as radio relay or rebroadcast). This makes sense given that Command is most closely associated with the human and activities in the cognitive plane. Given the current unease about robots conducting tasks within the Act function, it appears that the bulk of work for robot systems over the next decade will be primarily within the Sense, Shield, and Sustain functions.

OPERATIONAL FUNCTION	TOTAL ASSOCIATED TASKS	UNSUITABLE FOR ROBOTS	SUITABLE FOR ROBOTS (NEXT 3–20 YEARS)
Command	48	45	3
Sense	35	28	7
Act	44	14	30
Shield	21	7	14
Sustain	55	39	16
Overall Total	203	133	70

Figure 2.6.1: DGLCD Task List c. 2010

PART SEVEN – DEFINING THE CAPABILITY REQUIREMENTS

The preliminary PRICIE analysis conducted below is a tool used by capability developers to more fully examine the Army capability deficiency. Considerations for robot systems capability development (CD) work must be bounded by certain criteria. These criteria include, but are not limited to, the ability to operate in a complex warfighting environment; the ability to be integrated with other army systems; endurance, robustness, and survivability; simplicity and versatility; and reduced mass, volume, cost, and signature.²²² The following analysis must be reviewed and updated throughout the CD process.

7.1 PERSONNEL, LEADERSHIP, AND INDIVIDUAL TRAINING

Despite their moniker, the employment of unmanned systems will always be dependent upon interaction with human beings. As technological capability surges forward, humans will become ever more reliant on their unmanned

222. Fielding, "Robotics," 106.

robotic counterparts. This ever-maturing relationship between humans and technology will bring with it significant impacts on military personnel, leadership, and individual training.

7.1.1 PERSONNEL

The introduction of robot systems has the potential to broaden the recruitable cohort of the Army. Tele-operated robots will displace many soldiers from forward areas, putting the human operator further to the rear and out of harm's way. For this reason, general computing skills or dexterity with a remote controller—e.g., joystick, touch screen, or Wiimote™—will be more important for a tele-operator than will physical fitness or robustness. The value sets and degrees of mental, psychological, and emotional resilience required for military service will need to be the same for the remote tele-operator as for any close combat or close engagement soldier. Thus, the paradigm of the 25-year-old athlete as the most desirable soldier has the potential to change.²²³ A talent for violent computer games may yet become a highly prized asset.²²⁴

That is not to say that high-school dropouts with a penchant for first-person shooter games will become the soldiers of the Army of Tomorrow or the Future Army. New recruits must be adept at managing system complexity and will therefore need to be more intellectually capable and even better educated than before.²²⁵ As research continues into developing human-robot interfaces (HRI) that will allow one operator to control multiple robotic platforms simultaneously, the type of operator the Army needs must be more cerebral than previously required. To be sure, gains made in developing more intelligent personnel coupled with advances in HRI and robot control stations will eventually decrease the required number of human operators needed to operate distributed robot systems.²²⁶ Further down the road, a shift toward steadily increasing degrees of autonomy will generate the need to merely monitor, not control, these systems.²²⁷ That may eventually translate into a requirement for even fewer personnel, but it will also mean a need for soldiers with even higher levels of cognitive function to meet the demands associated with information and knowledge management. Unless the robotic platforms are self-sustaining—

223. Cowan, *Theoretical, Legal and Ethical*, 3.

224. Fielding, "Robotics," 107.

225. Donnithorne-Tait, "Unmanned Systems," 24.

226. McDaniel, *Robot Wars*, 54.

227. Barrett, "Testimony."

i.e., can repair and recover themselves, or other robotic systems are designed to do this—then it is more likely that the human resources that were formerly employed as front-line troops will instead be required to perform the rear area tasks of ensuring that the robotic platforms are kept operational. The information technology (IT) system manager will likely have a critical role in carrying out these tasks. Thus, there may not be an overall reduction in the number of personnel required, just a shift in where they are employed.

Even if robots alleviate human resource pressures, they may well simply increase pressures in other areas (such as maintenance and communications). How these pressures will balance is unknown at this time, and further research in this area will be required during subsequent CD work. Jim Hewitt of DSCEM provides an important lesson from the Canadian naval experience that the Army should draw on in terms of capturing labour costs associated with the implementation of new technologies:

The personnel aspect of remote systems has been the Achilles heel of naval underwater ROVs. Three underwater ROV systems: the SMARTADS (1980–1983), the MANTA (1988–1993) and the IRMDS (2003–2009) were projects where the equipment was procured to budget and timeline for the purpose of providing initial capability and training personnel. In all three cases the equipment performed up to or beyond specification and in all three cases the equipment was taken out of service because of manpower costs. This was despite the fact that in all three cases, the systems provided a capability at a lower capital cost, lower manpower cost and at a reduced operating cost than alternatives or in-service equipment. The problem was an irrational expectation that ROVs should provide a capability at no risk (technical or to personnel) at virtually no additional operating cost and at no manpower increase. The slight manpower and operating increases in order to initially introduce the equipment, while legacy systems remained in service, was deemed to be too much to bear. Any new technology always requires some increase in manpower and additional operating cost during the initial phase of the transition, unless it is decided to prematurely dispose of the predecessor capability and put all hopes on the new technology being just right, a very high risk action.²²⁸

228. Hewitt, "Comments."

Beyond recruiting, training, and career management, policies will need to be radically changed to improve the capacity of military personnel to use information. Though automation can help, there will be a need to get beyond the use of mediocre software tools to the cultivation and sustainment of a more intellectually sophisticated military force.²²⁹ Operating high-tech military equipment requires long-service professionals, not short-term conscripts.²³⁰ The robot systems team—which includes operators, battlespace managers and officers—will be most effective through relevant experience gained in an operational setting. A high turnover of highly skilled IT professionals will not be the desirable personnel situation for the robot systems team.

Advanced HRI and more capable control stations coupled with ever-increasing autonomous levels of operation will mean fewer personnel required to execute more tasks. On-board AI will be capable of processing reams of sensor and situational data, thus streamlining intelligence-analysis tasks and allowing the same number of analysts to be effective over a greater area.²³¹ Although automating platform operations will decrease the need for people to crew them, the need for personnel to maintain the systems is likely to increase.²³² Maintenance of robotic systems will likely not demand new trade structures, though it will certainly put pressure on the logistics branch to generate more multifunctional mechanics. This will need to be the focus of further study.



229. Gentry, "Doomed to Fail," 101.
230. Boot, "The Paradox," 28.
231. Fagan, "Testimony," 3.
232. DoD, *Roadmap 2009–2034*, 39.

addressed here: an emerging type of operational stress injury suffered by persons who are directly contributing to combat operations but are wholly removed from physical danger. It will need to be addressed before the transition from unmanned combat support and combat service support to actual robotic combat can be considered. Killing without risk is psychologically very difficult and changes the nature of warfare itself. The experience of armed Predator UAV pilots today seems to show that they suffer from higher levels of stress than jet pilots who fly combat missions.²³³ The stress of fighting a war thousands of miles away, then minutes later joining your family at the dinner table, presents mental health challenges that we need to understand better.²³⁴ Some would assert that a switch to an entirely automated warfighting mechanism may be the only way to alleviate this type of stress on humans.²³⁵ However, this type of emotional disengagement would likely just cause stress associated with the problem of moral responsibility for killing.

7.1.2 LEADERSHIP

Robots present both dilemmas and potential solutions in terms of personnel. The same is true for leadership. Clearly, ground-based robot systems will remain under the control of humans, perhaps for the next several decades.²³⁶ However, even with the transition toward fully autonomous operation, there will always be human leaders who plan the operational employment of robotic systems and oversee and monitor tactical execution. Culturally, there will be stresses in the future created by a potentially significant decrease in the numbers of personnel in the close combat trades.²³⁷

The notion of autonomous robotic subordinates will present leadership challenges to officers charged with planning and overseeing their employment. Beyond the legal responsibilities associated with accountability for the actions of robots, there will be a challenge to the concept of military ethos. Some writers say that if there is no risk to the leader on the battlefield then the leader's activities are conducted without honour. That seems to imply that one's perception of importance and honour is related to the level of exposure to risk.²³⁸ Although standoff is something militaries traditionally look to

233. Institut für Religion und Freiden, *Interview with Armin Krishnan*, 23 November 2009. 29 July 2010: http://www.irf.ac.at/index.php?option=com_content&task=view&id=306&Itemid=1.

234. Tierney, "Testimony."

235. Institut für Religion und Freiden, *Interview with Armin Krishnan*.

236. McDaniel, *Robot Wars*, 27.

237. DoD, *Roadmap 2009-2034*, 39.

238. Makin, *Future Warfare*, 46.

achieve, individuals fighting from remote locations could always take comfort in knowing that they were not only destroying an adversary but also protecting a peer fighting on the ground in close combat. This changing idea of what standoff means will present challenges to military leaders. What does it mean today when “drone” has become a colloquial word in Urdu and when Pakistani youth listen to rock songs that talk about America not fighting with honour?²³⁹ These issues are worthy of further examination.

An important distinction for leaders will be whether or not subordinate robot systems will be wholly reliant on human decision making or whether they will make decisions on their own based on the leader’s intent. The use of remotely operated systems presents the least concern to leaders. The success of remotely operated systems to date has already socialized the Army to their potential for mission effectiveness. Taking a lesson from the US Air Force, some think that human intervention will always be present while operating unmanned robotic systems. In the future, serving as a virtual pilot for an unmanned aerial system will be as prestigious as being an actual pilot today, though there is some concern over the interim impact of unmanned aerial systems on self-esteem in pilot culture.²⁴⁰ The same effects are likely to be encountered in the Army, but that will also require further study. In order for Army culture to embrace robots, humans must come to trust robot performance.²⁴¹ Army leadership will be responsible for socializing subordinates but in turn will also require socialization.

Autonomy offers a greater concern to leadership culture. Not surprisingly, younger soldiers often accept new systems more readily than more senior personnel, seeing them as new, exciting, and challenging. Raised on video games, they may see the operation of autonomous systems as natural and exciting.²⁴² To accept and trust autonomous systems, human operators need to be able to understand their reasoning process and the factors that precipitate certain actions. The machine needs to be able to communicate the reasoning behind its actions in an unambiguous manner that is also accessible to non-technical personnel—in other words, to explain itself.²⁴³

239. Singer, “Testimony.”

240. McDaniel, *Robot Wars*, 23.

241. Fielding, “Robotics,” 106.

242. Hanon, *Robots on the Battlefield*, 3.

243. Jerry L. Franke et al., *Holistic Contingency Management for Autonomous Unmanned Systems*, Lockheed Martin, 29 July 2010. <http://www.atl.lmco.com/papers/1344.pdf>, 61.

Moreover, in terms of autonomous computer decision making in determining how and where to employ lethal force, officers will likely insist upon direct communications with robots for such an application.²⁴⁴ Autonomous systems should therefore be programmed to request further intent or direction from leaders as opportunities for the application of force present themselves.²⁴⁵

Another area requiring examination is the proper ratio of soldiers and civilians in the future battlespace. The American experience in Iraq today shows that robot systems maintenance and sustainment is overwhelmingly—as much as 75 percent—outsourced to private contractors, including controversial firms like Blackwater.²⁴⁶ The rapid incorporation of robotics into the US Army has unduly strained existing maintenance structures, creating a need for more support from private contractors. Leaders will need to find a way to foster Army culture while potentially seeing much of the traditional work of the Army fall to robots and contractors. An implementation plan that is deliberate and phased will alleviate potential pressures on the leadership community (and, of course, the logistics branch).

7.1.3 INDIVIDUAL TRAINING

The impact on individual training caused by the introduction of robot systems must be light to moderate. Of course, any robot will bring new training requirements at the individual level, but proper guidelines and principles for capability developers will help minimize the amount of training required and the degree of associated difficulty. This will be discussed more fully in the “Equipment and Support” section below.

Efficiencies can be gained by leveraging existing competencies within Army military occupational structures. The knowledge, skills, abilities, and competencies necessary to operate, repair, and maintain robots and robotic components of large systems are generally similar to the personnel skill sets required to operate and repair electronics, computers and networks, avionics, and wheeled and tracked vehicles.²⁴⁷

The vision of the Army Engineering Branch for their development of individual training packages for remotely operated EOD robots at Canadian Forces

244. Nardi, *Autonomy*, 49–50.

245. Department of the Army, *Robotics Strategy White Paper*, 25.

246. Singer, “Testimony.”

247. Department of the Army, *Robotics Strategy White Paper*, 25.

Base Gagetown provides a brilliant illustration of potential impacts. The difficulty the branch experienced in maintaining knowledge and skill sets of both robot operators and maintainers needed to be remedied through contractor support for a train-the-trainer mechanism.²⁴⁸ Driven by high turnover at the EOD School, the staff there enables effective EOD robot training by maintaining close relationships with business and industry. This gives them the built-in flexibility they need to deliver mobile training teams to other bases when required. For other branches where the introduction of robotic systems looms, this type of equipment training team or even self-paced training may initially suffice for most training requirements.²⁴⁹

As with most other technologies, training on the operation and maintenance of robot systems and components must begin well prior to their use in an operational environment. Some soldiers may train on robot systems as part of their initial entry training in the Army. Continuation training on these systems will ideally be conducted at home bases.²⁵⁰ Such training can be greatly enhanced by the use of simulation. Today, most simulators for robots are not sophisticated enough to give real value, in either the operator or maintainer training mode, but that is improving. Often simulation training seems to be an afterthought, and little project money is left for it. Simulators should be developed in parallel to the real robot—maybe even before the robot vehicle is actually built.²⁵¹

7.1.4 EDUCATION AND PROFESSIONAL DEVELOPMENT

Professional military education (PME) can help leaders make the transition to the wider adoption of robots in several ways. Firstly, exposure to legal and ethical concerns associated with robot systems can help develop critical thinking and military cultural understanding by offering a novel concept to frame intellectual discussions. Giving leaders the opportunity to derive conclusions about the ethical employment of unmanned robotic systems will help alleviate fear of the unknown and help the Army become socialized to the systems. The US Army War College has already introduced robots in its curriculum with a view to informing leaders about the potential effects of autonomous systems.²⁵²

248. DCSEM, *Explosive Ordnance Disposal*, 14.

249. Department of the Army, *Robotics Strategy White Paper*, 23.

250. Department of the Army, *Robotics Strategy White Paper*, 22.

251. Hewitt, "Comments."

252. Nardi, *Autonomy*, 48.

Secondly, using robot technologies in staff courses geared to junior and senior officers will help build leaders' capacity for understanding how robots might best be employed in different situations. That will also encourage progress toward innovative development of tactics, techniques and procedures while at the same time driving novel future concepts for robotic systems capability developers. Students at the US Naval War College are today engaged in serious contemplation of how technology will alter the battlefield in the form of a potential robotics revolution.²⁵³ The Army will have to adopt similar PME objectives and strategies.

It should also be noted that partnerships with the civilian academic and technical collegiate community could be leveraged for educational purposes. The University of North Dakota charters a four-year degree program in unmanned systems piloting.²⁵⁴ There will likely be an increase in Canada's civilian curriculum offerings focused on the ethical and technical aspects of the growing robotic presence in human society, which the Army will be able to take advantage of. Canadian colleges and universities are already working in close partnership with DRDC. Robotics courses are offered at numerous institutions, including the University of British Columbia, Simon Fraser University, the University of Toronto, McGill University, the University of Sherbrooke, and the University of New Brunswick.

7.2 RESEARCH AND DEVELOPMENT AND OPERATIONAL RESEARCH (PLUS EXPERIMENTATION)

Some argue that the single greatest impediment to the development of robotics applications for land warfare at this time is not the limits of technology, but rather the lack of guidance from the military on the way in which robotics might be useful in the military context.²⁵⁵ Research and development (R&D) and operational research (OR) will ultimately guide the incorporation of robot systems within the Army as they provide the means to overcome technological limiters and inform force employment concepts through experimentation and analysis of existing data. Simply put, technological limiters will be overcome through iterative research processes funded by appropriate financial resources invested in the aforementioned priority areas. That said, the more guidance that the Army can give as to what systems it requires in the future, the better equipped researchers will be to focus their work.

253. Jackson, "Testimony," 2.

254. Tierney, "Testimony,"

255. Fielding, "Robotics," 101.

7.2.1 R&D PARTNERSHIPS

It is likely that much of the technology on the battlefield of tomorrow will be either directly or indirectly developed by the United States.²⁵⁶ Canada must therefore maintain its governmental, industrial, commercial, and academic partnerships south of the border. More specifically, DRDC will need to continue its current practice of leveraging American scientific and technical expertise by sharing its own resident capacity. However, to ensure successful support of R&D efforts to the Army, capability developers will have to inform DRDC as to the conceptual vision for robot systems employment. Sharing information regarding detailed future operating concepts or capability requirements will not only lead to research that is more focused and more relevant but will also serve to assist capability developers with understanding the opportunities for success and the potential limitations on the technological roadmap.

Other partnerships within the Department of National Defence (DND) will be essential for success as well. After all, DRDC is not strictly an Army resource, and there are probably areas where collaboration at the joint level will present opportunities for R&D efficiencies—especially in the area of autonomous intelligence—that will have equal application across the Land, Air, and Maritime environments. Indeed, DRDC is already actively engaged in joint collaboration. A lesson learned from the American experience is that lack of collaboration between the Air and Land environments in particular has greatly hindered the forward momentum of several unmanned systems projects. Environment-centric requirements and funding and ineffective collaboration were key factors that limited the ability to achieve commonality among subsystems, payloads, and ground control stations.²⁵⁷ Early collaboration ensures streamlined research processes and enables platforms to be acquired and fielded more quickly.

Given that robot systems generated for use by the Army will include not only UGVs but also UAVs, it is clear that close partnership with Air Force capability developers will be necessary. More significantly, it is likely that novel capabilities could be achieved by getting these systems to cooperate and collaborate with each other—i.e., by heterogeneous robot teaming. The US Department of Defense requires all force elements to identify and document in their acquisition

256. Makin, *Future Warfare*, 10.

257. Michael J. Sullivan, "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform," *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010; http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136, 3.

plans and strategies specific areas where commonality can be achieved between disparate environments.²⁵⁸ For both operational and fiscal reasons, it is imperative that DND adopt a similar approach. Academic partnerships represent a meaningful way of streamlining R&D processes. As mentioned, Canada has already recognized this, and DRDC operates in close conjunction with a number of university partners both within Canada and externally.

During the course of the RMS-Technology Demonstrator Project (1999–2003), DND (DRDC Atlantic and the Navy) partnered with industry to build an advanced remotely operated mine-hunting system. One of the signal successes of that project was the “Build a Little—Test a Little” (BaL-TaL) approach. This allowed problems to be solved logically, with complexity being built in as the work advanced. This type of approach significantly reduced overall project risk and was the main reason why the project was delivered on time and on budget. In the process of framing how future Army-sponsored R&D projects for UGVs/UAVs could be managed, the BaL-TaL approach with industry should be considered, especially where a significant technological advancement is required, posing several different problems and requiring a variety of technical expertise. One of the criticisms levelled at the BaL-TaL approach was that the project did not set high enough goals. However, several previous naval projects had set goals too high; few of them resulted in workable systems and none came in on time or within budget. Setting up limited but carefully targeted expectations, with clearly defined exit ramps if needed, and increasing the technical goals incrementally, proved to be a winning strategy, especially when working with a limited budget and avoiding the re-invention of the wheel.²⁵⁹

7.2.2 TECHNOLOGICAL RESEARCH AND DEVELOPMENT (R&D)

R&D focused on overcoming the many technological limiters associated with robot systems is charging forward at an accelerating pace. In the US and Canada, the massive spending and research that is taking place will eventually result in the ability to take the human out of the loop, thereby enabling unmanned robotic systems to operate autonomously.²⁶⁰ At DRDC Suffield, there is a full team of researchers—the Autonomous Intelligent Systems Section—dedicated to that very goal. Though some ethicists argue that such

258. Weatherington, “Testimony,” 3.

259. Thanks again to Jim Hewitt for the BaL-TaL concept. See Hewitt, “Comments.”

260. McDaniel, *Robot Wars*, 76.

research will inevitably result in permitting robots to locate their own targets and destroy them without human intervention,²⁶¹ there can be no doubt that humans now and in the future will control both technological development and subsequent employment of all robotic systems. However, immediate value can be created through research on autonomous intelligence for applications other than simply killing. Current international research on UGVs is mainly focused on perception and sensing technologies, integration of robotic systems with each other and with humans, human-machine interfacing and planning, on-board artificial intelligence for robotic systems, and platform-related technologies (including, but not limited to, weaponization).²⁶²

Given the omnipresence of improvised explosive devices (IEDs), ever-increasing amounts of R&D are being directed toward attacking that threat. Research in autonomous driving capabilities is one area of technological research that goes beyond the conventional sense of attacking the IED network. Autonomous driving would greatly limit the threat IEDs pose to humans along main supply routes while at the same time freeing up more soldiers for other tasks. As discussed previously in the section on technological limiters, autonomous driving for UGVs is a much more complicated proposition than it is for UAVs and maritime surface and underwater vehicles, given the complex nature of the land environment.

Some advocate that robot systems R&D prioritize the development of perception technologies needed to achieve autonomous mobility.²⁶³ Indeed, that is one of the many areas in which research is being conducted at DRDC Suffield. Research areas include waypoint navigation, obstacle avoidance, point-and-click to drive, miniature multi-axis scanning LIDAR (or LADAR), stereo vision and obstacle detection systems.²⁶⁴ Currently most perception systems build upon ranging sensors (LIDAR and stereo vision), since the geometric approach simplifies the identification of hazards and obstacles. Machine/computer vision approaches are used sparingly, as their generalized object-recognition ability is extremely limited. Unfortunately, geometric representations have limitations, the most significant being the inability to represent terrain far ahead of the vehicle while the vehicle is moving. This myopia limits the maximum speed at which the vehicle can safely travel.

261. Noel Sharkey, "Grounds for Discrimination: Autonomous Robot Weapons" *RUSI Defence Systems*. (October 2008): 87. 29 July 2010. <http://www.rusi.org/downloads/assets/23sharkey.pdf>.

262. Cowan, *Theoretical, Legal and Ethical*, 13.

263. Board on Army Science and Technology, *Technology Development*.

264. Nguyen, et al., "Land, Sea, and Air," 2.

Hybrid approaches that learn the relationships between imagery and geometry in real time are currently viewed as a potential solution to this problem. (DRDC Suffield terms this “learned trafficability.”) Obstacle avoidance is a key focus of current R&D efforts but, despite many advances, is not yet mature in terms of operationally ready UGV systems. Before those UGVs ever make their way to employment within the Army, they must demonstrate the ability to provide a level of safety and ability equivalent to comparable manned systems.²⁶⁵ Although not achievable today, suitable advances in perception technologies are likely in the next decade if R&D efforts remain focused on autonomous mobility.

Research on unmanned systems is also being conducted in other areas, including inertial navigation, laser-based simultaneous localization and mapping (SLAM) techniques, and GPS techniques that maximize the accuracy of localization in any situation, such as loss of GPS in so-called urban canyons.²⁶⁶ Current research also includes mapping multiple buildings to create neighbourhood maps, traversing stairs and other urban obstacles, and mapping in three dimensions.²⁶⁷ Again, these are simply research areas that are being explored; they are not really representative of current capabilities. What these research areas do have in common, however, is that each of them has a multitude of applications which the Army should be positioned to exploit the moment the technological readiness exists.

Research activities for manned counterparts in the areas of communications, alternative energies, and propulsion mechanisms all have applications in the unmanned robotic systems domain but need not be discussed in detail here.

7.2.3 OR/EXPERIMENTATION

A growing body of knowledge exists that can be exploited for operational research (OR). This includes both Canadian and American expeditionary and domestic successes and failures as well as opinions and attitudes relating to the incorporation of robots into human systems. The Canadian experience can provide data pertinent to UAVs and EOD UGVs. One potential area for OR may be the ideal usage of UAVs for the Army given that advanced satellite technologies and Tier 1 and 2 UAV systems may already provide necessary

265. DoD, *Roadmap 2007–2032*, 4.

266. Nguyen, et al., “Land, Sea, and Air,” 2.

267. Nguyen, et al., “Land, Sea, and Air,” 2.

ISR capability. Perhaps a look at UAVs that can readily enter urban structures could provide one potential avenue of exploration for experimentation.

Some contend that land-based robots can provide operational advantage only when employed offensively and that during the conduct of defensive or stability operations they will likely provide only minimal advantage.²⁶⁸ Such conjecture need not be a reason for accepting or rejecting the future robots. OR can offer a sound scientific basis for analyzing existing data, formulating relevant hypotheses, and providing proof through operational analysis and realistic experimentation across the continuum of operations. OR can also aid in using data analysis and experimentation to recommend potential platform and force structure tradeoffs.²⁶⁹ Conducting concept demonstrations and field experiments with promising technologies will also allow for early assessment to help define realistic requirements that are underpinned by sound operational concepts.²⁷⁰

The best use of OR will likely be the establishment of clear priorities for R&D. That would be based upon an evaluation of competing technologies (using simulation or seminar war games) in order to determine which solutions or combination of solutions offers the greatest potential capability benefit.

7.2.4 SIMULATION

Critical to the overall robot development strategy is the improvement of simulations that realistically model operator task load and projected capabilities of both tele-operated and autonomous UGVs. In the absence of significant numbers of prototypes to use in field exercises, simulations are the next-best tool to help predict the optimal use of these future capabilities and determine potential operational and strategic implications.²⁷¹ Better simulations will also contribute significantly to helping predict operational and strategic effects beyond immediate tactical employment considerations. Until numerous capable prototypes are available for use in the field, realistic simulations remain an important tool in defining how robots can contribute across the spectrum of conflict and in different environments.²⁷² DRDC Suffield develops and tests autonomous capabilities, using simulations, before transferring the software to the physical platform.

268. Winslow, *Unmanned Vehicle Robotic Warfare*, 26.

269. Department of the Army, *Robotics Strategy White Paper*, 23.

270. DoD, *Roadmap 2007–2032*, 3.

271. Nardi, *Autonomy*, 4.

272. Nardi, *Autonomy* 53.

7.3 INFRASTRUCTURE, ENVIRONMENT, AND ORGANIZATION

The incorporation of the Sperwer UAV system resulted in significant changes to both infrastructure and organizational structure. The question of whether or not robots will have limited impact on infrastructure and organizational structure within the Army of Tomorrow requires further analysis. As more and more systems are incorporated into the Army with broader usage and more autonomy, there will likely be a demand for changes to extant organizational structures. Such change in the future, however, will be entirely contingent on actual operational successes. Environmental degradation associated with the employment of robotic systems is no greater than that associated with their manned counterparts. In fact, unmanned technologies could be applied in various ways to spill detection, monitoring, and cleanup activities.

7.3.1 INFRASTRUCTURE

For the most part, existing infrastructure can be used to support integration of emerging robot systems. However, without divestment of some current capabilities, it is highly likely that incorporating significant quantities of robotic platforms will exceed the capacity of current infrastructure, such as storage space. For example, the Canadian Forces EOD School is now responsible for all remotely operated EOD vehicle training, including storage and maintenance of associated robotic training aids.²⁷³ Existing line unit storage facilities may be sufficient for robots, which contain many of the same components as manned systems and therefore require the same storage conditions and preventative maintenance as any other vehicle system, including mechanical and electronic systems, sensors, weapons, and communications. No special or unique facilities are required for security, maintenance, or storage of robotics systems, though there may be a requirement for increased storage space. Capability developers and project management offices will need to ensure that existing infrastructure for secure storage and routine maintenance is made available as required.²⁷⁴

Beyond garrison storage and maintenance infrastructure, there will be a need to ensure that the existing mobile sustainment capacity of field units is also used to support a robot fleet. It is not foreseen that any type of special infrastructure will need to be erected to support individual or collective training events beyond current practice.

273. DCSEM, *Explosive Ordnance Disposal*, 14.

274. Department of the Army, *Robotics Strategy White Paper*, 26.

7.3.2 ORGANIZATION

Effects on organizational structure arising from the integration of robots should be minimal. There should be no requirement for special robotic schools or robotic units in the Army of Tomorrow. That is not to say that there is no scope for a robot support platoon in the order of battle of a field unit, though such a structure will be undesirable in the near term. As mentioned, there may be a requirement for specialized robot systems operators in the future but, again, such developments are not expected in the coming decade. For now, robot operation will be an all-arms function.

A recent coordinated review in the US indicated that although no new military occupational specialties (MOSs) are needed for robotics in the near term, future requirements may emerge for new MOSs if the cumulative effect of many fielded robots demands it.²⁷⁵ The establishment of common robot design criteria and insistence upon user-friendly human robot interfaces will minimize unique training demands and should negate consideration of new MOSs in the Army.

The US Army is embedding unmanned aerial systems in all its Brigade Combat Teams.²⁷⁶ The same is true of today's Canadian expeditionary battle groups, with corresponding impacts on the composition of artillery organizations, both garrisoned and deployed. For unmanned aerial systems that are force generated by the Army, further research must be conducted to determine which organizations are best suited to this kind of incorporation. And in terms of UGVs, all field units must be prepared to take advantage of the benefits offered by robot integration.

Any evaluation of the costs and benefits of current or emerging robotics systems must be accompanied by an analysis of the impact that such systems may have on Army organizations. A modification to organizational structure can be the result of efficiencies gained through the introduction of robotics systems into the force or can be a necessary by-product of the system without any apparent increase in efficiency.²⁷⁷

Using the Air Force experience as a guide, it is easy to see how the development of the UAV led to the creation of dedicated UAV flights where pilots fly their

275. Department of the Army, *Robotics Strategy White Paper*, 23.

276. Weatherington, "Testimony," 5-6.

277. Department of the Army, *Robotics Strategy White Paper*, 21.

aircraft from networked ground control stations. The question must be asked: Is such a paradigm shift possible in the conduct of land operations? Is it foreseeable that an infantry sub-unit commander could remotely operate a company from a distance? Beyond the Army of Tomorrow horizon, it is possible that independent unmanned ground reconnaissance, sustainment, or engineering organizations (section or troop level) will be technologically possible, even desirable. It will be inconceivable to shift to such organizations in the future without slowly incorporating user-friendly robotics technology into existing structures across the Army today.

However, the relative explosion in the employment of robot systems in the US in support of that country's expeditionary operations has demanded the stand-up of a dedicated maintenance and repair facility. The Joint Robotic Repair and Fielding (JRRF) is staffed by reservists, Department of Defense civilians, and contractor support personnel.²⁷⁸ Without the JRRF, the US Army in Iraq would not have the availability of robots that they currently enjoy. Canada's Army cannot look to adopt such a structure any time before the Army of Tomorrow, but it remains a possibility for the Future Army. Fiscal constraints alone would prohibit the procurement, in the foreseeable future, of a sufficient quantity of robotic systems that require their own maintenance organization.

In terms of strategic structures, the Army would be well advised to designate a robot systems manager akin to an LCMM to coordinate R&D and acquisition of Army UGV systems. That person would be the Army's principal advocate for UGV systems and might logically be situated in CADTC.²⁷⁹ He or she would ensure the presence of corporate memory, preventing bad ideas from being repeatedly attempted, and would also ensure that support teams are provided with adequate resources to train personnel to operate and maintain the equipment.²⁸⁰

7.4 CONCEPTS, DOCTRINE, AND COLLECTIVE TRAINING

Because robots have the potential to revolutionize military operations, it is imperative that doctrine is developed with respect to how these systems will be employed, how they fit together, and how they integrate into the overarching

278. DoD, *Roadmap 2009–2034*, 38.

279. Similar suggestions for the US DoD can be found in the Board on Army Science and Technology, *Technology Development*; and Nardi, *Autonomy*, 4.

280. Hewitt, "Comments."

network. With the notable exception of the US Army, most military robotics authorities tend to agree that the potential doctrinal impacts of the use of robots must be examined. The history of warfare tells us that every new leap in technology, whether it was the English longbow, the tank, or the atomic bomb, outpaced existing strategy and doctrine for its employment. The same thing appears to be happening now with the push for rapid technological advances in robotics.²⁸¹ The successes of Lightning War ought to serve as an example to capability developers that the use of robots must not be regarded in the same manner as a mere vehicle or tool upgrade.

The battlefield, which has been becoming less crowded for centuries, might empty out even more as small belligerent units try to conceal themselves from ubiquitous friendly sensor networks, emerging only briefly to launch lightning strikes before going back into hiding.²⁸² Robots will certainly play a role in supporting the rapid aggregation of friendly forces that will be required to neutralize these enemy groupings in the Army of Tomorrow.

Although currently there is no established doctrine guiding the employment of robots, it must be accepted that the importance of doctrine will increase proportionally with the capability, utility, and presence of robot systems on the battlefield.²⁸³ Considering that capability will be directly proportional to the sophistication of AI governing system behaviour, strategic planners need to get ahead of the technological curve. There appear to be at least two primary directions in which the doctrine of robot systems might go, and there is some tension between them.²⁸⁴ The two main tactical operating concepts are the mothership concept and the swarming concept.²⁸⁵

7.4.1 MOTHERSHIP CONCEPT

This concept, borrowed from the US Navy, envisions a ship deployed at sea that acts as both a carrier and a C2 node on the network. Once in location,

281. Singer, "Wired for War?" 105; Deputy, *Counterinsurgency and Robots*, 16; Crispin, "What Killed," and Cowan, Theoretical, Legal and Ethical, 2.

282. Boot, "The Paradox," 29.

283. Deputy, *Counterinsurgency and Robots*, 2–5.

284. Singer, "Wired for War?" 105.

285. The current concept of unmanned systems integration in the United States Army is based on the systems being classified as equipment, which inserts them into the planning process at the force planning or tactical level (see Deputy, *Counterinsurgency and Robots*, 13). It has been stated that the addition of unmanned and robotic systems to the force will simply increase the efficiency and effectiveness of human roles that are already well established in doctrine (see Deputy, *Counterinsurgency and Robots*, 15). "There is no capstone Army doctrine for the use of robotics systems in the contemporary operating environment, nor is there a need for one." See Department of the Army, *Robotics Strategy White Paper*, 19. This statement has generated concern that the US Army is looking at robotics as simply equipment upgrades. American industry executives have been quite vocal as to the requirement to consider doctrine, ostensibly because they know that a robotics roadmap is most likely to survive budget cuts if it is underpinned by a sound doctrinal vision.

the ship can then autonomously deploy its payload of smaller boats, UAVs, and/or submarines in accordance with its mission. If the ship is clearing sea lanes of mines, it might pack onboard a set of mine-hunting robotic mini-sub; if the ship is patrolling a harbour, it might carry mini-motorboats that would scatter about, inspecting any suspicious ships; or, if it needs to patrol a wider area, it might carry a few UAVs.²⁸⁶

For land operations, the mothership would be a tele-operated or semi-autonomous UGV linked to higher headquarters via the network and probably having the appearance of a standard infantry carrier. Once a suitable location in its area of operations is found, the mothership would drop ramp and release its payload of smaller UGVs and UAVs into the environment. The subordinate vehicles would carry out their missions semi-autonomously or in fully autonomous mode while exchanging information with the mothership.

The mothership would provide the headquarters with a picture of the environment and allow for centralized control of the robots at its disposal. The mothership itself would provide adequate control of the autonomous robotic systems, but would also restrict the robots from reaching their full combat potential due to communications and signals requirements required to link to the mothership.²⁸⁷ This tactical concept is not without disadvantages:

The concept of motherships comes with a certain built-in irony in that it entails a dispersion, rather than concentration, of firepower ... If you look at nature's most efficient predators, most of them don't hunt by themselves: they hunt in packs; they hunt in groups.²⁸⁸

7.4.2 SWARMING CONCEPT²⁸⁹

The main doctrinal concept alternative to motherships is called swarming. Rather than being centrally controlled, swarms are made up of highly mobile, individually autonomous parts.²⁹⁰ In a pattern similar to the way German

286. Singer, "Wired for War?" 106.

287. Deputy, *Counterinsurgency and Robots*, 12.

288. Singer, "Wired for War?" 108.

289. The self-organization of these groupings is a key to how the whole works. The beauty of the swarm, and the reason why it is so appealing for unmanned war, is the way it can be made to perform incredibly complex tasks once each part is programmed to follow incredibly simple rules.

For example, rules for flocking, a complex swarming behaviour exhibited by birds, are simply separation, alignment, and cohesion: (1) Separation: Don't get too close to any object, including other robots; (2) Alignment: Try to match the speed and direction of nearby robots; and (3) Cohesion: Head for the perceived centre of mass of the robots in your immediate neighbourhood. See Singer, "Wired for War?" 108–109.

290. Singer, "Wired for War?" 108.

wolfpacks operated in the Battle of the Atlantic, individual platforms disperse across the battlefield conducting information-gathering activities and searching for opportunities. Those opportunities might be collection of data pertinent to a commander's critical information requirements or even effects-based activities. Once a few platforms lock onto an item of interest (as previously programmed in priority by a human systems or operations manager), they signal others in the nearby area to converge. Once they gather the desired information or achieve the desired effect, the swarm then disperses to continue its mission. Individually, each member of the swarm is weak, but the overall effect of the swarm can be tremendously powerful.²⁹¹

Rather than driving a single tele-operated UGV into a building and manoeuvring room by room to see if an enemy is hiding there, a soldier could let loose a swarm of tiny robots that would scramble out and automatically search on their own.²⁹² An important consideration here is the idea of aggregate complexity versus individual complexity. A single robot must be highly complex (and therefore expensive), because it must perform its task without assistance. A swarm, on the other hand, can be made up of many simple (and therefore cheap) robots that cooperate in such a way as to create an aggregate or collective complexity.

Advantages of the swarming concept include the ability to mass firepower while maintaining survivability.²⁹³ This concept is the opposite of the mothership concept in that motherships employ centralized control mechanisms and disperse firepower.²⁹⁴ Swarms may not be predictable to the enemy, but neither are they exactly controllable or predictable for the side using them. That unpredictability can lead to unexpected results. Instead of being able to point and click and get the immediate action desired, a swarm takes action on its own, and that may not always happen exactly where and when the human commander wants it.²⁹⁵

Micro-robotic swarms (or robo-flies) of low-flying UAVs could be used in the future military battlespace, for surveillance (or more broadly for ISR functions) in confined indoor spaces, or for urban warfare, where higher-flying UAVs or satellite-based sensors may not be effective.²⁹⁶

291. Singer, "Wired for War?" 108.

292. Singer, "Wired for War?" 109.

293. Attacking a swarm has been described as going after bees with a sword. See Singer, "Wired for War?" 110.

294. Singer, "Wired for War?" 109.

295. Singer, "Wired for War?" 110.

296. Stocker, *Autonomous Intelligent Systems*.

Once committed to a task, the swarm would not need further communication, guidance or control until the mission was accomplished. The swarm would disperse and collect in a given area depending on its ability to detect and close with a given target or objective. Through simple commands and programmed logic, the swarm would react almost instantaneously, allowing little time for enemy reaction.²⁹⁷ Swarm intelligence provides insights that can help human controllers manage highly complex systems that range from only several unmanned robotic systems to hundreds of unmanned robotic systems under the supervision of one human operator.²⁹⁸

Warfare and technology writer Max Boot contends, “Large concentrations of troops and weapons are targets for destruction, not marks of power and in the future they no longer will exist. Military units, to survive, must not only be small, but highly mobile, self-contained, and autonomous.”²⁹⁹ Though humans may also be used to swarm, it may be practical and more advantageous to have the robots do it.

7.4.3 DOG CONCEPT

A third, less prevalent, potential tactical force employment concept for robot systems is known as the dog concept:

The dog model of robot theoretical integration portrays robots as man’s best friend. A robot would be paired with a human in order to compl[e]ment human capabilities ... In [this] model robots would be an extension of the combined arms concept ... The dog model would mitigate risk to the information operations line of operation by ensuring that a robot supporting counterinsurgency operations would never be seen without a human companion charged with the same mission ... Direct accountability and supervision would be emphasized in the dog model.³⁰⁰

The dog model is something of a reality today with the Boston Dynamics Big Dog robot, a manoeuvrable unmanned logistics system capable of carrying soldier equipment across all terrain. The futuristic dog concept would see a Big Dog-like companion that not only carries a soldier’s kit but also acts as a

297. Deputy, *Counterinsurgency and Robots*, 12.

298. McDaniel, *Robot Wars*, 57.

299. Boot, “The Paradox,” 29.

300. Deputy, *Counterinsurgency and Robots*, 12.

fire team partner, sensor platform, and communications relay. It might also be regarded as a much-scaled-down version of the current DARPA MULE project.

The dog concept, like the mothership and the swarm, involves teaming, which has two components: teaming between robots and teaming between humans and the robot systems. Human-plus-robot teams will always present a unique challenge: how to develop robot systems technologies to enable the human to predict, collaborate, and develop trust with the robot teammate.³⁰¹

7.4.4 OTHER POTENTIAL CONCEPTS

The three concepts described above do not describe the only potential doctrinal employment of robots. For the foreseeable future, robots will continue to fill roles in an “equipment sense” rather than a “systems sense” where robots fill niches in accordance with TTPs. The wholesale doctrinal changes outlined above are put forward in preparation for the advances in autonomous operation that will be seen during the long-term timeframe. Those advances will potentially lead to many other employment concepts.

What will not change is that, for UGVs to be effective in the future battlespace, they must be able to work both autonomously and in teams. They will need to share data and be able to run semi-autonomously if tele-robotic connections are broken.³⁰² What will change in the future will be the potential for robots to introduce new sense capabilities and methods of effects projection.

Currently there are many UGV-UAV team concepts where the two work together and share information for accurate target identification, acquisition, and hunting.³⁰³ DRDC Suffield is currently conducting research in that area. Prescribed for the future are very small and subtle ghostly systems, which will be capable of entering small spaces with immense sensory capability and substantial firepower.³⁰⁴ In the future as well, the environmental boundary as it is currently understood may become more artificial, opening up tremendous potential for the development of robots that can operate across physical environments. One can imagine, for example, a robot that can fly or swim to a site, conduct its reconnaissance on the ground, and then return to the sea or the air in order to relay its collected data.³⁰⁵

301. DoD, *Roadmap 2007–2032*, 51.

302. Winslow, *Unmanned Vehicle Robotic Warfare*, 27.

303. Winslow, *Unmanned Vehicle Robotic Warfare*, 28.

304. McDaniel, *Robot Wars*, 31.

305. Fielding, “Robotics,” 103.

The most revolutionary UAVs are the smallest. DARPA is working on aerial vehicles the size of an insect or a hummingbird that can hover undetected and perch on a telephone pole or a window ledge. Some models have no wings at all; others use flapping, bird-style wings. They are designed to be cheap enough that they could saturate a battlefield with sensors, thus delivering the swarming capability previously discussed.³⁰⁶ Projects for the more distant future include nuclear-powered UAVs that can fly at 70,000 feet and stay on station for months or even years at a time; a UAV aircraft carrier that could serve as a mothership for launching and recovering smaller UAVs; UAV tankers that could refuel other UAVs in flight; and vertical-takeoff UAV cargo-carriers that could supply troops in a combat zone.³⁰⁷

There is also the concept of using robots as precision munitions, for “putting warheads on foreheads.”³⁰⁸

Imagine the psychological impact on a commander who learns that the enemy has just released 10,000 multi-environment “assassination robots” programmed to locate, identify, and assassinate him. (This is a good reason why we may want to be careful with managing and securing biometric information). Each of the targets has a unique signature. Robots like as these may be the next generation of precision munitions—in fact, this is the area of robotics that has the single greatest potential for changing the way we fight.³⁰⁹

It is in this respect that unmanned robotic systems can be viewed as offensive force multipliers where one human systems manager can be the nexus for initiating a large-scale unmanned robotic system attack from the ground and the air.³¹⁰

Indeed, just as the optimum operating concept for tanks turned out to be combined arms units, robot systems concept choices may also mix and mingle. The dog, swarm, mothership and other concepts can be blended, and human commanders can be inserted at the key decision points, such as the point where swarms start to cluster.³¹¹

306. Boot, “The Paradox,” 24.

307. Boot, “The Paradox,” 24.

308. McDaniel, *Robot Wars*, 32.

309. Fielding, “Robotics,” 103.

310. McDaniel, *Robot Wars*, 77.

311. Singer, “Wired for War?” 110.

7.4.5 COLLECTIVE TRAINING

At tactical levels, leaders must understand how robotics systems can most effectively support their operations. This understanding can be gained through collective training. Leaders must integrate robotics systems into operational planning much like any other enabling system and must plan for support and replacement in the event that the systems are destroyed or break down. They must be capable of integrating robotics systems into the full suite of live, virtual, and constructive training means available to small units and must integrate them into unit training plans and strategies. Leaders will need to understand how and when robotics systems best support their operations in different environments, cultures, and missions.³¹²

In order to achieve a measure of success in collective training, field units will need to have access to robotic systems while garrisoned, as the development of TTPs at levels two and three will ultimately ensure meaningful collective training at level four and beyond. Ideally, the integration of robotics into unit training and exercises will occur long before embarkation on the Road to High Readiness.

Another requirement is that commanders and staff be given the opportunity to plan for and employ robots during collective virtual exercises prior to conducting field training exercises. Army Simulation Centres must therefore be equipped with the proper supporting software tools, applications, and models to allow planners to incorporate robotic systems.

7.5 INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY

An ambitious objective for the Future Army would include the development of better onboard sensors that could see through walls, foliage, or soil; cheaper, more pervasive systems that could provide 24/7 coverage of the battlefield; better data compression and transmission techniques that could allow more digital bits to be sent much faster; and more powerful computers that might make it possible to create, for example, a real-time, three-dimensional model of a city showing all the people who reside in it.³¹³ Ongoing research on such modelling is being conducted at DRDC Valcartier. For the Army of Tomorrow, tele-robotic systems will probably make up the majority of deployed robot

312. Department of the Army, *Robotics Strategy White Paper*, 24–25.

313. Boot, "The Paradox," 27.

systems. When it comes to these tele-operated UGVs, the weak link is communication systems.³¹⁴

A key concern for the future of robotic systems will be network bandwidth and integration. It is imperative that robot systems be able to operate at extended ranges, receiving input from the network via secure communication links and processing data using sufficiently powerful onboard AI. There are two takeaways for capability developers: (1) the communications problem presented below needs to be solved if reliable tele-operation is ever to be achieved; and (2) onboard AI must be sufficiently powerful (and morally, legally, and ethically robust) to sense (observe), analyze and evaluate (orient), decide, and act on its own in the event of the inevitable failure of network communications. Therefore, planning for communications disruptions is paramount in UGV development.

Functional areas relative to the communications problem include unmanned systems network integration and radio frequency (RF) performance such as range, data rate, latency, environmental conditions; spectrum coordination; information security; and interoperability with the network.³¹⁵

7.5.1 THE COMMUNICATIONS PROBLEM

Although there are scenarios where the use of tethered robotics (robots that are hardwired to their control station via copper or fibre-optic cables) may be acceptable, it is generally preferable for robots to operate free of the physical restraint of network cabling. Liberated from a wired connection, the system will require secure, persistent, high-bandwidth communications with its control station facilitated by compression algorithms that allow both (1) the upload of reams of sensor data for subsequent processing by the network; and (2) the download of high volumes of information from the network for processing by the system's onboard AI. Although the ideal operating mode involves higher degrees of autonomy in order to ease network throughput congestion, the communications problem cannot be totally alleviated. The most brilliant of autonomous systems will still require persistent connection to the network in order to maintain situational awareness—in this respect, robots are no different than humans.

314. Winslow, *Unmanned Vehicle Robotic Warfare*, 34.

315. Nguyen et al., "Land, Sea, and Air," 9.

The EOD community traditionally worked with tethered robots during the conduct of domestic police work. Police organizations have long since transitioned to wireless EOD solutions as a way of achieving greater control of the robot and greater standoff from the explosive device. Military EOD organizations have similarly adopted a preference for wireless solutions.³¹⁶ But the ease of manipulation and enhanced standoff achieved through RF-based control comes with disadvantages.

How deep into the battlespace would we want to control robots? As far as possible?³¹⁷ Over open terrain, robots can be controlled from a distance of more than a kilometre using the same ultra-high-frequency (UHF) communications that ground stations use to control UAVs. UHF transmissions, however, require line of sight between transmitter and receiver. For that reason, close terrain—especially urban terrain—represents a significant challenge for the transmission of UHF signals. Given that robotic missions will certainly involve operation in an urban environment, an alternative to UHF control will be necessary. The challenge is that increased bandwidth for a signal is directly proportional to the ease with which that signal can be blocked. Communications technology researchers have come up with many novel solutions to the urban signals problem, but they have not yet found an optimal solution. The urban environment is not the only terrain currently presenting a challenge: at the NATO IST-089–affiliated European Land Robotics Trials, tree cover had a significant detrimental impact on systems that required continuous, reliable communications.

Satellite-based solutions are promising, but until the chronic shortage of available satellite access is solved, they do not represent a viable research area. Research here will begin only when there is substantially cheaper access to space and orbit.³¹⁸ The spectrum in which robot systems communicate must evolve past radio frequencies and exhibit an agility to hop around in the spectrum to ensure robust, secure communications.³¹⁹

Radio control in an urban operational environment is, to say the least, challenging. The US Army's former bomb-disposal robot, the Vanguard, has been largely scrapped due to its total inability to operate under the cluttered

316. Nguyen, et al., "Land, Sea, and Air," 9.

317. Fielding, "Robotics," 106.

318. Hew, *The Generation 9*.

319. DoD, *Roadmap 2009–2034*, 27.

electromagnetic spectral conditions of an operational theatre.³²⁰ Transmitting signals clearly through urban environments is a technical problem that has yet to be solved.³²¹

Not only must robots be designed to be sensitive so that they can receive low-powered signals in an urban environment, they must also be sufficiently shielded to prevent electromagnetic attack. The communications infrastructure itself is likely to be an early target for enemy attack, and success in such attacks could disable all robot forces.³²² System effectiveness will be optimized only if robots have sufficiently powerful onboard AI to understand whether or not the mission should be aborted given the inability to communicate with the network. As mentioned, more onboard intelligence also means less demand for data-link capacity.³²³

Fundamental physical limits (speed-of-light, horizon line-of-sight, and occlusion) will result in round-trip signal delays that will limit the feasible range for effective remote control.³²⁴ Accordingly, there will be an increased focus on moving to systems that rely less on network input and more on onboard processing—this is the primary driver for the shift to autonomous systems.

7.5.2 INTEROPERABILITY

Interoperability is the ability to operate in synergy in the execution of assigned tasks.³²⁵ It includes universal network connectivity as well as simplified support considerations such as training and logistics. Interoperability is achieved by buying common components, systems, and software and/or by building systems to common standards.³²⁶ However, caution must be exercised to ensure that interoperability does not create a system that is so uniform that a single cyber attack method could take it down in its entirety. Heterogeneous components that abide by standards would offer a better solution to this problem (the World Wide Web is a good example of such a system).

Operations conducted by the Army of Tomorrow will be performed in a fully networked JIMP-enabled environment. Robot systems can be effectively

320. Crispin, "What Killed."

321. Crispin, "What Killed."

322. Sparrow, "Killer Robots," 68.

323. McDaniel, *Robot Wars*, 47.

324. Hew, *The Generation*, 6.

325. DoD, *Roadmap 2007–2032*, 13.

326. DoD, *Roadmap 2007–2032*, 13.

integrated into operations only if data, computing, and communications infrastructures are designed with high degrees of interoperability.³²⁷ The desired degree of interoperability will be achieved when all systems communicate on the same integrated network, populating and drawing on common databases, all within a joint and international framework. Interoperability with coalition partners will also help alleviate concerns with respect to identification, information gathering, and legal issues.³²⁸

For seamless interoperability, the network must allow information to flow freely among all nodes and terminals using a common communication format and protocol, comparable to the TCP/IP protocol and the graphical interface format (GIF) that was implemented on the Internet to allow PCs and Macs to communicate.³²⁹ It will be essential for Canada to continue its participation in standards development through the NATO Standardization Agency (such as STANAG 4586, 4660 and 7085) and other relevant partnerships, including close liaison with the American-led Joint Architecture for Unmanned Systems (JAUS).³³⁰

7.5.3 LATENCY

When a robot receives an input signal, it processes the signal in order to generate an appropriate output. The time it takes to perform the processing is referred to as latency. It is latency that causes a human operator to click multiple times when only one click is required (which incidentally contributes to even more latency). It is also part of the reason why all computers have a tendency to act strangely every once in a while.³³¹ Latency is an important issue that has led to the abandonment of some robotics projects. The armed SWORDS robot was shelved by the US Department of Defense because of problems associated with the way the robot responded to commands: it would either ignore orders completely or act them on only after a delay. The lag between the button being pressed and the robot responding was sometimes as great as eight seconds.³³² Overcoming latency is an important design consideration for any unmanned robot system, especially one that is armed.

327. Donnithorne-Tait, "Unmanned Systems," 22.

328. McDaniel, *Robot Wars*, 79.

329. Hanon, *Robots on the Battlefield*, 8.

330. DoD, *Roadmap 2007-2032*, 14.

331. Crispin, "What Killed."

332. Crispin, "What Killed."

7.5.4 SOFTWARE

According to some estimates, an experienced programmer unknowingly inserts approximately one mistake into every ten lines of code.³³³ The consequences of software defects in robot systems may prove deadly, especially as higher degrees of autonomy and lethality are achieved. The legal concerns relating to the issue of defects may lie between the matter of software quality and other factors such as cost, ease of use, or time required to bring the technologies to market.³³⁴ It must be accepted that any robot will suffer from occasional glitches related to software defects. Defects can be greatly mitigated, however, by resisting the temptation to hurry systems into the field force before they are operationally ready. Robots that are capable of applying lethal force cannot be rushed.

Software programmers must be guided by the principles of interoperability and modularity. Robot systems must be compliant with the software communications architecture of the Land Command Support System (LCSS) or whatever command support system exists when the robotic systems are brought into service. Software and subsystem design should be as modular as possible, in order to enhance operational flexibility, component re-use, interoperability, and standardization.³³⁵

7.5.5 ENCRYPTION

Encryption is the primary method of ensuring communications security and integrity. But it is a double-edged sword when encryption also greatly limits robot range, since encrypted signals must be received fully and strongly in order to be acted upon.³³⁶ This will make it unacceptable to deploy robot systems on the ground that do not use encryption, as communications security is the primary means of preventing adversaries from penetrating unmanned systems.

7.6 EQUIPMENT AND SUPPORT

Robot systems consist of a manoeuvrable platform (including robot chassis and mobility apparatus), robotic subsystems (including protection, power,

333. McDaniel, *Robot Wars*, 67.

334. McDaniel, *Robot Wars*, 67.

335. Donnithorne-Tait, "Unmanned Systems," 22.

336. Crispin, "What Killed."

communications, temperature control, etc.), and the mission payload itself (sensors, weapons, lasers, manipulator arms, etc.) together with its associated control equipment. Equipment and support are important considerations in ensuring effective cohesion of the overall robot system.

7.6.1 HUMAN ROBOT INTERFACE (HRI) AND CONTROL UNITS

Robot systems present the same HRI issues to the military user as the employment of sophisticated communication systems in the battlespace, such as display representation, ergonomics, orientation, environmental protection, security, and hardening.³³⁷ In short, the interface needs to be easy to use and understand. The desired end state would be a user interface that is completely transparent and gives the operator a feeling of being in direct contact with the robot.³³⁸

Whether controlling tele-operated robots with human speech, pen-based gesture commands from a small handheld personal digital assistant, or even a Wiimote, the bottom line is that control must be intuitive and user-friendly but also free of ambiguity.³³⁹ One way to ensure this is to design one unit that can be used to control the operation of any robot. Optimizing the control of multiple types of vehicles from a single control station would also serve to minimize training across host platforms and to minimize logistical support requirements.³⁴⁰ The Multi-Robot Operator Control Unit (MOCU) is an example of a graphical operator-control software package that allows simultaneous control of multiple heterogeneous robot systems from a single console.³⁴¹ A MOCU-like device should be pursued by robot systems capability developers for employment within the Army.

7.6.2 RUGGEDIZATION

Robots must be robust enough to withstand elements of the natural environment and be resistant to machine wear and tear and physical shocks. Although commercial off-the-shelf components will have to be used for R&D and prototype testing, fielded systems should be no different than their manned counterparts. Special attention must be paid to ruggedization

337. Donnithorne-Tait, "Unmanned Systems," 24.

338. McDaniel, *Robot Wars*, 68.

339. Trebes, "Agile Robotics," 102.

340. DoD, *Roadmap 2007-2032*, 50.

341. Nguyen, et al., "Land, Sea, and Air," 6.

requirements. It makes no sense to field a robot with a heavily armoured chassis that is designed to withstand bomb blasts and also be easily repairable if the mission package mounted on that chassis is neither.

7.6.3 POWER CONSIDERATIONS

Some have insisted that the desired end state for power generation should be 72 hours of continuous operation without refuelling or recharging batteries.³⁴² Such considerations will need to be weighed against the type of UGV, its task, and its mission environment. Another requirement should be that power generation systems, whether fossil-fuel-fired generators or some other source, be equipped with some sort of noise-suppression system. Selection of an energy source for the system is important, as it will be an important factor in achieving requisite scaling of mission duration and system size, weight, and power.³⁴³

7.6.4 SPARING

By the very nature of the employment of unmanned systems, robots will be sent into high-risk environments. Therefore, damage that cannot be repaired locally will probably be commonplace. Robots deployed with American infantry units and EOD teams sustain significant battle damage; soldiers and units that evacuate their robot for repair need to have confidence that it will be repaired or replaced with a robot from a common pool of spares.³⁴⁴ Therefore, sparing is an important equipment consideration. The number of spares needed will depend on the amount of risk that each robotic platform is subjected to. For example, expeditionary operations in non-permissive environments will require more spares than a school, a collective training centre, or a home-unit quartermaster.

7.6.5 MAINTENANCE AND LIFECYCLE MANAGEMENT (LCM)

First- and second-line maintenance for robotic systems will follow standard CAF maintenance policies and procedures just as is being done today with the Dragon Runner™ and tEODor systems.³⁴⁵ Requirements for contractor support personnel can be alleviated through intelligent design practices and by exploiting depot repair teams. The ultimate goal is to make robots as

342. Nguyen, et al., "Land, Sea, and Air," 5.

343. Department of the Army, *Robotics Strategy White Paper*, 23.

344. Department of the Army, *Robotics Strategy White Paper*, 24.

345. DCSEM, *Explosive Ordnance Disposal*, 14.

maintenance-free as possible.³⁴⁶ In the future, there may be a shift in Army doctrinal TTPs: maintenance organizations may be required to patrol the battlespace to recover and repair robots rather than having the crew or unit bring the system to a centralized maintenance site.³⁴⁷

PART EIGHT – FRAMEWORK FOR ROBOT SYSTEMS³⁴⁸

Robots employed by the Army may be sorted into two broad categories: unmanned ground vehicles (UGVs) and unmanned aerial systems—of which unmanned aerial vehicles (UAVs) currently make up the majority. All of these units are currently tele-operated. Anticipated technological advances will see systems with continually increasing levels of autonomy that are capable of tasks of greater complexity in ever more diverse and challenging operating environments. Those systems will be capable of carrying out any task within the land environment, though certain tasks will still have to be performed by humans. Robots will be produced by commercial developers in all shapes and sizes, will be powered by all manner of fuels and propulsion mechanisms, and will employ the gamut of mobility technologies. Some will be lighter than a feather while others could weigh more than a tank. In order not to find itself behind the technological and production curve, the Army must develop a framework that facilitates a shared understanding with concerned partners that will foster the CD process by identifying Army requirements.

A framework can also serve to focus R&D efforts. When it is combined with the principles and considerations outlined in the PRICIE analysis, S&T researchers will have the appropriate information they need to concentrate efforts in appropriate areas.³⁴⁹ For a researcher, it can become difficult to envision robot systems requirements or specifications when there is a lack of a common language between the people who conceive the systems, those who design them, and those who actually build them. Given the increasing number of robotics applications, distinct environmental terminologies and classifications have the potential to become too broad to remain meaningful.³⁵⁰ A unifying framework would help bridge such gaps in understanding.

346. Department of the Army, *Robotics Strategy White Paper*, 24.

347. Department of the Army, *Robotics Strategy White Paper*, 24.

348. The framework option described in this section was updated in the fall of 2010. The latest framework, much like the definitions found in Part Two, will be updated upon publication of DLCD's Robot Concept Paper in winter 2010.

349. Nardi, *Autonomy*, 16.

350. Fielding, "Robotics," 101.

8.1 FRAMEWORK BUILDING BLOCKS

A robot system contains (among other components) a UGV platform, a UAV platform, or some combination of the two. Thus, the key start point in building the framework will be the provision that the platform around which the robot is built cannot contain a human operator. It may contain a human payload, but the operator of the system cannot reside on the platform itself.

If the platform does not operate on the ground, then it is an unmanned aerial system (or space system) or a maritime-based unmanned surface or underwater system. Unmanned systems in the air and maritime environments have existing frameworks, which will not be re-examined here as they are not pertinent to land operations. However, the classification of UAVs employed by the Air Force does include Tier Three UAVs that are generated and managed by the Army. That particular component of the UAV framework will overlap with the Army robot systems framework. This analysis will initially focus on UGVs and will tie in Tier Three UAVs at the end.

If unmanned ground-based platforms are incapable of locomotion (e.g., cannot manoeuvre to close with a target, cannot jockey for a better fire or observation position, or cannot move to avoid detection), then the platform may be regarded as an immobile or static unmanned system, such as an unattended ground sensor (UGS) or some other unmanned automated machine (a coffeemaker or landmine, for example). If the unmanned ground-based platform is capable of locomotion, then it may be considered an unmanned ground vehicle (UGV).

Starting with these macro considerations of unmanned systems, it is possible to classify UGVs generated by the Army into a meaningful framework. Existing frameworks tend to focus on size and weight as the definitive robot characteristics. Before assuming that classifying systems based on physical dimensions is the best methodology for building a framework, it is worthwhile to ask why size matters. For example, size does not matter when it comes to range, as those two parameters, size and range, can be directly or inversely proportional. Perhaps the only thing that matters is how size affects either the performance of a robot's primary role or task or the way the robot moves from one place to another.

If the UGV is not small and light enough to be carried by an individual soldier—without human enhancement—then it will be considered an

Intermediate or Large UGV. On the other end of the dimension scale, if the UGV cannot be seen with the unaided human eye, it is classified as a Micro UGV. Micro UGVs will likely be the subject of future research and development once technology opens up new operating environments in the nano or quantum realms. If the UGV is somewhere between the two ends of the dimension scale, then it will be classified as a Small UGV. Small UGVs are well suited to supporting light or dismounted forces.

Thinking of size in terms of portability is helpful, as it allows us to visualize the robot system in question. Portability and mobility considerations are important when considering the supported force. If a UGV is too heavy to be carried by a soldier (i.e., it has larger dimensions than a Small UGV) yet has insufficient mobility to support a mechanized force, then the UGV can be termed an Intermediate UGV. Intermediate UGVs are therefore suited to support roles for light or dismounted forces but are not man-portable. UGVs that can manoeuvre in support of mechanized forces may be considered Large UGVs.

The next step in developing a framework must be an examination of the tasks that UGVs may perform. An analysis of doctrine, battle task standards, and TTPs relevant to the unique branches, arms, and corps reveals a seemingly endless list of potential functions, missions, and tasks within the paradigm of land operations. Tasks are therefore too specific to build into a framework without creating the impression of a need for countless niche systems. Rather than looking at potential tasks individually, it is more appropriate to examine logical groupings of tasks where multi-role systems could be employed. The robot systems framework will look at groupings of tasks according to the doctrinal framework of the operational functions. In this respect, robots may be grouped according to where they lie within the operational functions of Command, Sense, Act, Shield and Sustain.

The operational function of Command includes tasks such as battle management (development of situational awareness and a common operating picture, information and knowledge management, etc.); technical communications and information systems support; and decision support tools. The Sense function includes tasks such as intelligence, surveillance and reconnaissance (ISR); mapping; CBRN and explosives reconnaissance and detection; and target acquisition and designation. The Act function includes the insertion of forces through manoeuvre; direct fire support; indirect fire support; and the application of non-lethal effects (electronic attack, influence activities, crowd-control operations, etc.). The Shield function includes tasks

such as counter explosive threat (explosive ordnance disposal, counter-mine and counter-IED); as well as counter-mobility and mobility support (some of these tasks may arguably fit under the Act function as well). Lastly, the Sustain function includes maintenance, replenishment, medical, and casualty evacuation tasks. The tasks listed here reflect current robot applications as well as areas of current research and experimentation. Such a list, however, will never be exhaustive; it will always grow, which means that any framework that includes classification by task will be ungainly. However, the operational functions are exhaustive and therefore represent a more suitable classification criterion.

The development of platforms which are modular in nature and therefore capable of supporting different operational function packages will be a key foundational principle of the robot systems framework. Indeed, it will be a key design principle. If effects are needed to support a particular organization in the Command and Sense domains, then it makes little sense to develop completely separate mobility technologies. A design goal within this framework will be one platform capable of plug-and-play operation in accordance with the operational function package required.

8.2 CLASSIFICATION BASED ON AUTONOMY³⁵¹

Different levels of autonomy for unmanned platforms require different supporting technologies and methods of integration with manned systems. Therefore, an examination of the level of robot autonomy—or, more specifically, the level of autonomy in the execution of a system’s primary task—is in order. Autonomy is generally broken down into three categories: tele-operation (remote controlled), semi-autonomous, or fully autonomous. These sub-categories can be further described as follows: tele-operated robots generally

351. “The ALFUS Detailed Model is a three-axis model where autonomy level is determined by the complexity of the missions that an unmanned system is able to perform, the degrees of difficulty of the environments within which the system can perform its missions, and the levels of operator interaction that are required to perform the missions. Mission complexity uses the metrics of: levels of sub-tasking, decision making, and collaboration, knowledge and perception requirements, planning and execution performance, etc.; human independence level uses the metrics of: interaction time and frequencies, operator workload, skill levels, robotic initiation, etc.; and environmental difficulty can be measured through obstacle size, density, and motion, terrain types, urban traffic characteristics, ability to recognize friends/foe/bystanders, etc.” See Hui-Min Huang, et al., *A Framework for Autonomy Levels for Unmanned Systems (ALFUS)*, Presented at AUUSI’s Unmanned Systems North America 2005, Baltimore, MD. June 2005. 29 July 2010: http://www.nist.gov/customCAF/get_pdf.CAFm?pub_id=824538, 5–6. “The ALFUS model then distinguishes ten levels of autonomy ranging from remote control to fully autonomous. Remote control is where the human operator, without benefit of video or other sensory feedback, directly controls the actuators of the system on a continuous basis, from a location off the vehicle and via a tethered or radio linked control device using visual line-of-sight cues. The most recent ALFUS definition for full autonomy is: completes all assigned missions with highest complexity; understands, adapts to, and maximizes benefit/value/efficiency while minimizing costs/risks on the broadest scope environmental and operational changes; capable of total independence from operator intervention.” See Hui-Min Huang, et al., *Autonomy Levels for Unmanned Systems (ALFUS) Framework: An Update*, Presented at 2005 SPIE Defense and Security Symposium, Orlando, FL. 29 July 2010: http://www.nist.gov/customCAF/get_pdf.CAFm?pub_id=822672, 8.

rely on the operator to sense the operating environment and control the performance of the robot in that environment; semi-autonomous robots, once deployed, are capable of performing some of their intended functions without human intervention; and autonomous robots, once deployed, are capable of performing all of their intended functions without human intervention.³⁵²

In order to be considered fully autonomous, a robot must be completely free of any human intervention. There will always be instances where a human could or should intervene despite the fact that a system can be regarded as fully autonomous (indeed, humans are no different in that respect). Therefore, it is necessary to prescribe the conditions in which human input makes a robot something less than fully autonomous. For the present framework, a system is considered fully autonomous if it can carry out its primary task without intervention by a human operator, even if a human manager may need to intervene in order to provide follow-up direction or clarification should the system encounter an unanticipated change to the situation. If a robot does not require persistent tele-operation by a human operator in order to carry out its task but is not sufficiently intelligent to make decisions without human input, it may be considered semi-autonomous.

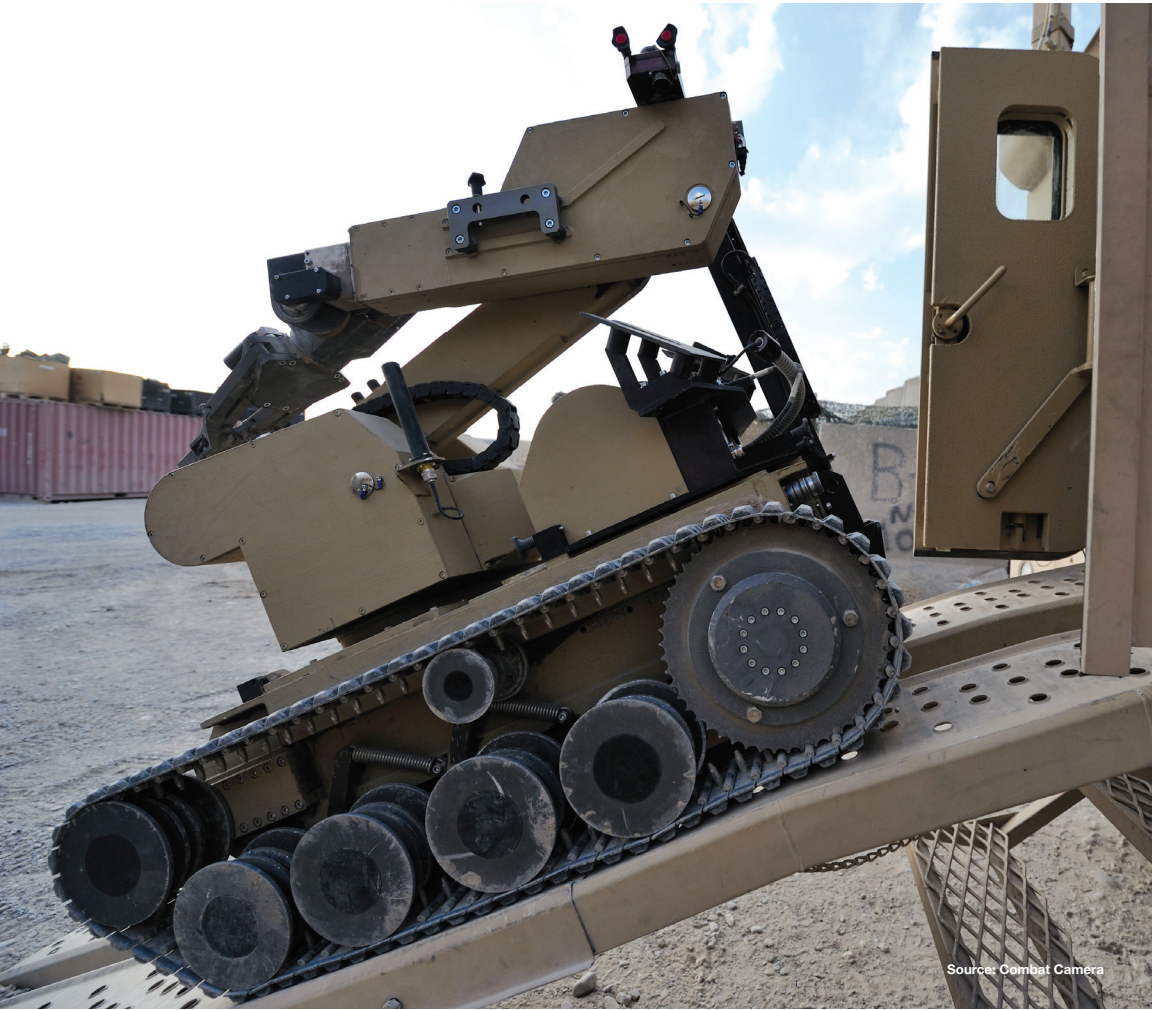
Levels of autonomy are generally defined by the time interval between human inputs/direction. Therefore, the least autonomous robot is the one that requires constant human input. This is tele-operation, where there is a human operator who manipulates and controls the robot from a remote location. Semi-autonomy is anything that lies between zero autonomy (constant tele-operation) and full autonomy—that is, robotic operation that is free of human input during the execution of the task (other than input in the form of command direction should there be a change in the situation, as already discussed).

These definitions fit well with DSTO-GD-0467, which states, “The central result is that it is not a question of whether a system ‘is’ autonomous or ‘has’ awareness, but whether it has ‘sufficient’ awareness to be ‘sufficiently’ autonomous for the situation at hand.”³⁵³ The DSTO paper goes on to describe three levels of autonomy: remote control (tele-operation), human in the loop (semi-autonomous), and fire and forget (autonomous). It uses the terms “dumb,” “smart,” and “brilliant” interchangeably with these three categories.

352. Fielding, “Robotics,” 100.

353. Also used by Hew, *The Generation*, 2.

The smaller the size and weight, the more manoeuvrable and inconspicuous the system is, and the less power is required for the platform. However—at the present time—as the size, weight, and power requirements for an unmanned platform are increased, greater varieties and degrees of autonomy and intelligence are possible (such as information sharing among distributed, networked, intelligent systems for collective intelligence, cooperation and collaboration and in stay time over a potential target, in decision making, and in additional offensive capabilities).³⁵⁴ In other words, current technology



Source: Combat Camera

354. Stocker, *Autonomous Intelligent Systems*.

supporting increasingly autonomous modes of operation requires increasingly large platforms in which to place it. Although this is a key concern today, Moore's Law will make this consideration much less important in ten years.

8.3 INDIVIDUALS AND SWARMS

In a military sense, swarming occurs when several units conduct a convergent attack on a target from multiple axes.³⁵⁵ Swarm robotics, however, refers to a multi-robot system in which large numbers of robots, each with very basic programming, interact with one another and with their environment in such a way as to demonstrate a desired collective behaviour. This complex swarm behaviour emerges from the simplest level of programming in each member of the swarm. Although an individual robotic platform may require many thousands of lines of code in its programming in order to generate a specific behaviour, a member of a swarm can be programmed with just a handful of simple rules that are meaningful only when that member is in the presence of the rest of the swarm. Because of the lower computing requirement, swarm robots can be much smaller and cheaper than their individual counterparts. Those differences demand that swarm robots and individual or stand-alone robots be differentiated within any robotics framework.

Because the intelligence of a robotic system can be extremely difficult to measure, as seen above in the footnote outlining the autonomy levels for unmanned system (ALFUS) criteria, it is not a useful classification parameter. Intelligence itself simply refers to too many different parameters and measurements. For example, if the most intelligent systems were classified as those that can operate as part of multi-component systems, that can communicate, interact, learn, and collaborate with other members of the same system, or with other distinct but compatible systems, and that are interoperable with, rather than controlled by, human systems,³⁵⁶ then the potential emergent intelligence of swarms would be marginalized.

For the purposes of the framework, it is sufficient to say that the robot's behaviour is based on either its own onboard intelligence or the emergent intelligence of a swarm.

355. Edwards, *Swarming and the Future of Warfare*, xvii.

356. Stocker, *Autonomous Intelligent Systems*.

8.4 FRAMEWORK

The Table at Figure 2.8.1 illustrates one possible robot framework for the CD community. This land-based framework, which includes the ground and the airspace immediately above the ground, is broad and all-encompassing. All told, it allows for the classification of 240 distinct types of robot systems.

An alternative option for a framework could be one that mirrors the system advocated by the US National Academy of Sciences. By focusing on system complexity alone, the academy was able to identify four categories of UGVs:

- Tele-Operated Ground Vehicles (remote-control robots);
- Semi-Autonomous Preceder-Follower Systems (smart or automated robots);
- Platform-Centric Autonomous Ground Vehicles (brilliant robots); and
- Network-Centric Autonomous Ground Vehicles (autonomous robots).

These classes represent increasing levels of autonomy, with each class having distinct technology needs.³⁵⁷ Within this system, tele-operated ground vehicles come in all sizes and work across all five operational functions. In this respect, the technology required to operate and support a remote-controlled EOD robot is no different from a tele-operated tank in a fire base. Semi-autonomous Preceder-Follower systems consist of Follower UGVs that navigate by chasing a beacon on a vehicle to its front and traversing the same pathway. Preceder UGVs contain a higher level of AI and therefore have more autonomy. They follow routes based on mission inputs and onboard technologies such as path-planning and obstacle avoidance. The Preceder UGV has a human manager who oversees its operation and can step in and help when required (i.e., the Preceder UGV has no ability to respond to changes in the mission).

A platform-centric autonomous ground vehicle is capable of carrying out an assigned mission once it gets its input from a human. This includes point-to-point mobility and completion of assigned tasks associated with its mission.

357. Board on Army Science and Technology, *Technology Development for Army Unmanned Ground Vehicles – Summary*, The National Academies, January 2003. *The National Academies Press*. 29 July 2010: http://www.nap.edu/catalog.php?record_id=10592.

ENVIRONMENT	SIZE	AUTONOMY LEVEL	OP FUNCTION	SYSTEM TYPE
Ground (G)	Micro (M)	Tele-operated (T)	Command (C2)	Individual (System)
Air (A)	Small (S)	Semi-autonomous or	Sense	Swarm (Team)
	Intermediate (I)	Partially autonomous	Act (Effects)	
	Large (L)	(P)	Shield	
		Fully autonomous (F)	Sustain	

Naming Convention:
 Unmanned is the prefix to all systems.
 Environment, size, and autonomy level are abbreviated by first letter.
 Op Function is always written out.

Examples:
 A remote-controlled tank would be classified as an Unmanned GLT Effects System.
 A group of autonomous miniature helicopters used for company-level ISR tasks would be classified as an Unmanned ASF Sense Team.

Figure 2.8.1 : Robotic Framework for CD Community

Network-centric autonomous ground vehicles are the same as their platform-centric counterparts except that they receive their inputs from the network. Therefore, they do not need the human to take network input and convert it into human understanding in order to create output data to send to the UGV as a machine input that will enable the desired machine output. The human is in effect removed from the loop, though still a part of the network. The difference is that the UGV receives network input and takes appropriate action to achieve the desirable machine output. Moreover, network-centric autonomous ground vehicles would include swarms.

These four categories could be mixed and matched to account for systems with mixed autonomous modes. They could be extended to Tier Three air platforms, thus creating eight distinct types of land-generated robot systems which would be capable of conducting missions across the five operational functions simply by adding an appropriate mission payload. Therefore, this framework more readily supports the principle of multi-mission capability. It also fits with the DRDC maxim that autonomous intelligent systems (AIS) must be distinguished from the unmanned platforms on which they may be mounted.³⁵⁸

The need for a common frame of robotic reference is paramount in order to move the robot agenda forward. Although both robot framework options are

358. Stocker, *Autonomous Intelligent Systems*.

workable, the first option may risk being overly complex. Further discussion is required between Army capability developers and the R&D community with respect to which framework ought to be implemented. Since both options presented are all-inclusive and borrow the best qualities of existing disparate frameworks, both are viable choices.

PART NINE – IMPLEMENTATION PLAN

For the Americans, robots represent the supreme method of casualty avoidance. For that reason, robot implementation has to date spanned all operational functions. Because robots offer the potential to save lives at a time when the US is losing so many soldiers, much of the US Army leadership is convinced that “any technology is good technology” and that the “time for fielding is right now.”³⁵⁹ As a direct result of the on-slaught of niche system introduction, the US capability development process is struggling to catch up. The *Department of Defense Unmanned Systems Integrated Roadmap* is an attempt to get ahead of the curve, but even it is simply a list of technologies with anticipated fielding timelines. The DoD still lacks an overarching concept to guide the introduction of new technologies.

Canada is not flush with capital. Therefore, the robot systems concept that stems from this study must be grounded in an implementation plan that makes operational sense and is also fiscally responsible. Considering that it has taken more than forty years to develop rudimentary UAVs that operate in a relatively simple operational environment, it should be understood that military technologists will face a daunting challenge to keep pace with any desired implementation plan for UGV systems.³⁶⁰

As mentioned previously, the actual introduction of robots within the Army has already occurred. Thus far, all robotics fielded in the land environment may be regarded as supporting equipment or tools filling niche roles and integrated exclusively with manned systems. Given the rapid advance of technology, robots will no longer be considered mere tools or equipment and therefore must be seen as the potential revolution in military affairs that they represent: robots will eventually transition from being tools to being team members. The rapid pace of technological change creates a very real likelihood that the capabilities and autonomy of unmanned and robotic systems will

359. Lefkow, *Gen Wants Unmanned Ground Vehicles*.

360. Trentini et al., *Autonomous Land Systems*, 9.

outpace the ability to properly integrate them into the force.³⁶¹ An implementation plan could be used as a roadmap, akin to the detailed vision put forward by the US Department of Defense. Rather than simply listing robots on timelines, however, the plan would serve as the foundational concept which would govern the logic behind the continuing CD process for robots in the Army.

Robotic implementation can be viewed in phases or waves.³⁶² The first wave usually consists of cheap and easy systems, experimental in nature, which allow units to develop workable TTPs. This wave socializes the force to robotics while buying time for the development of the more sophisticated second wave. The second wave is simply an evolutionary step serving to further socialize the force to newer technologies and capabilities while buying more time for the development of the third and final wave of robots. This third wave would consist of distributed fully autonomous networked systems.³⁶³ In addition to buying time for R&D and achieving the required degrees of socialization, a phased implementation also keeps capability developers firmly in control of the introduction of robot systems, allowing strategic planners to decide degrees of desired autonomy for given tasks based on operational success and the present state of technological readiness. It also gives time for international law to catch up.

A survey was conducted among American officers to find out how humans saw the implementation of robot systems unfolding. Although the survey participants lacked scientific and technical awareness, their responses helped form a picture of the relevant social underpinning, which may help capability developers understand what types of systems might be more readily accepted into the field force. Those surveyed guessed that countermine operations would be the first to go to the robots, followed by reconnaissance, forward observation, logistics, and then infantry. Oddly, among the last roles the respondents named were air defence, driving or piloting vehicles, and food service—each of which has already seen automation.³⁶⁴ The overall pattern—EOD and counter-mine, followed by ISR and logistics, and finally robots working within the Act function—will run through the implementation plan.

361. Deputy, *Counterinsurgency and Robots*, 7.

362. Crispin, "What Killed;" and P.W. Singer, "Robots at War: The New Battlefield," *Wilson Quarterly*. (Winter 2009) 29 July 2010: <http://www.wilsonquarterly.com/article.CAFm?aid=1313>.

363. Crispin, "What Killed."

364. Singer, "Robots at War."



Source: Combat Camera

Robot systems should be implemented in the Army in phases that mirror the CD horizons. The initial phase has already begun and consists of the further introduction (or spin-ins) of tele-operated EOD and ISR systems. In accordance with technological readiness levels, there are several technologies that can support immediate implementation of robot systems capable of EOD and ISR tasks. Given that the IED will likely be belligerents' weapon of choice for the next few years at the very least,³⁶⁵ it makes sense that the initial cadre of Army robots be capable of defeating that threat. Indeed, the existing cohort of Army robots—Dragon Runner™, Talon, and Packbot on the ground and the dynamic group of Tier Three UAVs in the air—is already geared toward defeating it. It is universally accepted that those robots are merely the first generation; they are the equivalent of the Model T Ford or the Wright Brothers' Flyer.³⁶⁶

However, further implementation of robots within Horizon One need not focus solely on counter-IED technologies. In order to socialize the broader force to robots, the use of robots will have to be expanded beyond their present stovepipes in the combat engineer and Air Force communities. It must also be noted that failures during this initial introduction of systems will likely set back the integration process by years while leaders regain trust in robotic systems that produced unintended and unanticipated consequences in lost time, money, or lives.³⁶⁷ The most conservative implementation scheme, then, stays the course in Horizon One, with the further introduction of tele-operated systems acting as direct extensions of the human.³⁶⁸

In the near future, ground-based robots with strike capability are not supportable. Persistent human intervention is unavoidable until the issues of liability, discrimination, and proportionality are resolved. The level of technology and the degree of artificial intelligence required to make necessary distinctions do not yet exist.³⁶⁹ Although these issues occupy a future horizon at this stage, non-lethal applications such as EOD and ISR offer the greatest potential for utility in the near term and are also likely to provide the greatest return on investment in the immediate future.³⁷⁰

365. Lefkow, *Gen Wants Unmanned Ground Vehicles*.

366. Singer, "Testimony."

367. Nardi, *Autonomy*, ii.

368. McDaniel, *Robot Wars*, 78.

369. McDaniel, *Robot Wars*, 80.

370. Fielding, "Robotics," 102.

It should be noted that the Army currently faces a challenge in getting the optimal mix of ISR capabilities. Because information dominance is universally recognized as the key to military success, a veritable glut of ISR systems has penetrated the land environment, with many more planned for the near future. As already discussed, unmanned robotic systems represent the ability to fill gaps in the present C4ISR system. More importantly, ISR is the task for which current technology is best suited. Therefore, the introduction of functional ISR robots will allow successful socialization sooner rather than later.

The second phase of robotic implementation will be concurrent with Horizon Two. Here, the integration of semi-autonomous ISTAR, logistics, and engineering systems will take place. Building on the successes of mature tele-operated technologies in the initial phase, this phase will see an even broader proliferation of systems as well as the first iterations of semi-autonomous systems. ISR and engineer systems, which were previously only employed through remote control, will now be given a measure of limited autonomy as they navigate routes and perform basic tasks under the supervision of a systems manager rather than under the control of a dedicated operator. Likewise, logistics systems that employ established technological preceder–follower technologies will be slowly integrated into convoy operations and all manner of echelon combat service support systems (to include technologies such as semi-autonomous carrier mules).

In addition, the application of robotics to the logistics domain in the warehouse setting will provide the defence community with an early example of how to use higher levels of autonomy in a relatively benign test environment.³⁷¹ At the same time as it implements technologies with higher degrees of autonomy in logistical settings, the Army will continue to use more proven semi-autonomous and tele-operated technologies in an operational setting. This will allow soldiers to be socialized to the advantages of robotics and will prepare the force for the integration of more autonomous systems in the long-term Horizon.

The relationship between the capabilities of robots, their assigned missions, and their presence on the battlefield is proportional: as their capabilities increase, so will the other two factors, leading to a greater number and diversity of systems on the battlefield.³⁷² It is inevitable that as technology improves, each branch or corps will see applications for robots in the

371. Trebes, "Agile Robotics," 104.

372. Deputy, *Counterinsurgency and Robots*, 6.

execution of their unique roles. So long as technologies are introduced with the intent of this implementation plan in mind, they need not be discouraged. The key is to not to get ahead of the technological curve: systems must not be introduced in the wrong environment or before they are fully capable. If they are, it may take a long time to recover from the backlash against further implementation. Therefore, the risk is not worth taking.

This implementation plan takes into account the fact that, over time, there will be growing demand for increasingly autonomous and increasingly lethal systems. However, if a deliberate approach is taken to introduction and integration, the value of robot systems can be established on an institutional level. The systems will be tested and fielded by younger personnel who are already familiar with robotic warfare in computer games and who will likely embrace the new technology enthusiastically.³⁷³ However, successful integration requires acceptance both by soldiers in tactical organizations and by higher-level leadership.

The final phase of robot integration will occur during the long-term Horizon. This phase will see the highest degrees of autonomy necessary for ISTAR, logistics, and engineering systems. It will also see the introduction of lethal effects systems. Weaponizing unmanned systems is a highly controversial issue that will require a patient crawl–walk–run approach as each application’s reliability and performance is proved.³⁷⁴ As previously mentioned, weaponization will be palatable only if trust is built first.³⁷⁵

What most military technologies seem to have in common is that they are all initially designed as surveillance systems. However, in a pattern that echoes the history of manned flight, UAVs such as the Predator were soon put to work attacking enemy positions.³⁷⁶ It would be naïve to suggest that UGVs will not one day contribute to this strike capability. Once robots establish a track record of reliability in finding the right targets through previously proven ISTAR applications, it will be acceptable to use them in a strike capacity. Some writers have said that, if the ISTAR function and tele-operated weaponization are optimized without mistakes or unintended consequences, then machines will eventually be trusted to do it all themselves.³⁷⁷ Such

373. Hanon, *Robots on the Battlefield*, 10.

374. DoD, *Roadmap 2007–2032*, 54.

375. Crispin, “What Killed.”

376. Boot, “The Paradox,” 23; and Deputy, *Counterinsurgency and Robots*, 3.

377. Crispin, “What Killed.”

assertions merely constitute speculation at this time and certainly would not be in the realm of the possible before the furthest reaches of Horizon Three. In any event, the evolution of autonomous systems within Horizon Three would certainly follow the same incremental approach: intelligence missions first, strike missions later.³⁷⁸

The three-phase implementation plan suggested above must proceed in lockstep with detailed operational research supported by rigorous experimentation and simulation, in order to ensure that the best ideas proposed here are properly advanced while others are likewise properly discarded in a timely fashion. This phased implementation, which involves the transition of robots from tools to team members, will underpin the subsequent writing of an Army Robot Concept.

PART TEN – CONCLUSION

As traditionally exemplified by Moore’s Law, technology is increasing at an exponential pace. With respect to robots, this pace of change represents both a challenge and an opportunity for the Army. As the force employment concept for the Army evolves toward adaptive dispersed operations (ADO), new technologies will be required for success. Unmanned systems in general, and robots in particular, can play a noteworthy supporting role as an enabling concept of ADO.

Today’s technology is able to support military operations through limited tele-operation tasks. However, increased R&D efforts built on joint and international partnerships that transcend military boundaries are sure to break down technological constraints and steer systems evolution toward the Army of Tomorrow requirement. Technology that supports increasing degrees of autonomous operation in engineering, ISR, and logistical systems will be ready in ten years. However, if the Army waits for autonomous technologies to be ready before introducing simpler robotic systems to the wider force, there will be a significant risk of disruption and distrust. The key is to socialize the Army to robots sooner rather than later, introducing them in an iterative and evolutionary manner only as they are ready, thus setting the conditions for success in the conduct of ADO and future force employment concepts.

378. Barrett, “Testimony.”

The full potential of robot systems will not be realized unless the technologies and what they can do are embraced wholeheartedly. Requirements must be set that challenge robot systems developers to realize the full potential of military robotics, and funding for their development must be sufficient to achieve that potential. Lack of ambitious goals or lack of enthusiasm and funding must not be allowed to eviscerate robot potential.³⁷⁹

Lastly, the scale of implementation should be acknowledged here. As a small army, Canada's Army does not have delusions of creating a multi-billion-dollar unmanned force equivalent to the roadmap adopted by the United States. DND's recent Dragon Runner™ contract provides an example of how much it can cost to field these technologies. For a system that is already well developed with mature R&D conducted within the US, each tele-operated EOD robot will cost about \$46,000. For four of them, the total contract amount is more than \$1.2 million, including training and other aspects.³⁸⁰ It is clear that, projected defence budgets simply cannot support a mass proliferation of niche systems. Therefore, it is imperative that resources expended in developing this capability be focused on systems that are modular and interoperable, thus allowing the institutional flexibility required to keep pace with technological change without wasting essential capital. The implementation process for this concept can be scaled to fit budgetary constraints. However, cutting out any phase of the overall plan would likely have undesirable consequences in the future. In order to determine exactly which robots make the best sense at which times, a rigorous scientific approach must be adhered to throughout the CD process. To make such a guess today would be premature and would risk setting the force up for a bad investment.

There is much work to be done before robots fundamentally change the nature of warfare. In the interim, these systems are and will be capable of conducting a broad range of tasks that will allow the Army to optimize its use of critical human resources while at the same time socializing the force to the future of operations, which assuredly resides with unmanned systems. The Army must work closely with its scientific partners to ensure the timely integration of technologically ready systems that fill existing capability gaps or bring measurable capability improvement.

379. Hanon, *Robots on the Battlefield*, 11.

380. See <http://www.casr.ca/doc-acan-eod-dragon-runner.htm>

CHAPTER 3

ARMY ROBOTICS CONCEPT: FROM TOOLS TO TEAM MEMBERS

Source: Combat Camera



“Whatever doctrine prevails, it is clear that the military must begin to think about the consequences of a 21st-century battlefield in which it is sending out fewer humans and more robots. Just as the technologies and modes of wars are changing, so must our concepts of how to fight and win them.”

—P.W. Singer, *Wired for War*

PART ONE – INTRODUCTION

Robots are beginning to have a significant impact on Canadian Armed Forces (CAF) expeditionary and domestic operations.³⁸¹ The use of robotics is a departure from more traditional methods of task execution and has begun to greatly enhance Army methods of intelligence, surveillance, and reconnaissance (ISR) and the generation of effects through target acquisition (TA) and remote strike capability. However, with the exception of certain niche tasks, such as explosive ordnance disposal (EOD) and chemical, biological, radiological, and nuclear (CBRN) operations, the bulk of Army unmanned capability has been limited to the skies, where a plethora of unmanned aerial vehicle (UAV) systems has extended the range of Army sensing and allowed for ever-increasing levels of standoff. Drawing on the success of such aerial systems, this study will examine how the Army should maximize the use of land-based robots to augment its effectiveness into the future.

Land-based robots face considerable operating challenges due to the complex and dynamic nature of the land environment. Today, humans remain better able to perform the vast majority of tasks associated with the conduct of land operations. However, this situation is expected to change in the future when technological improvements give robots the capability to keep pace with—and even outperform—human soldiers. Therefore, ground-based robots are expected to become key technological enablers that will enhance the execution of adaptive dispersed operations (ADO).³⁸² Robots will serve as force multipliers, providing a presence where humans cannot and performing tasks for which humans are not required in order to realize mission success. Thus, robots will allow optimum employment of human resources in mission-critical tasks such as close engagement of the population—an activity that will remain personnel-intensive and unsuited to robots. Most other tasks, across all five operational functions, could be done by or with the help of robots.

PART TWO – FROM TOOLS TO TEAM MEMBERS

Today, robots offer tremendous utility as tools, providing assistance for military tasks that are well suited to automation or considered dull, dirty, or

381. For this concept, robots are defined as unmanned, reprogrammable, multifunctional mobile platforms (complete with manipulators) which are designed to move material, parts, tools, or specialized devices such as sensors through various programmed and "sense and respond" actions for the performance of a variety of tasks in both structured and unstructured environments.

382. ADO is the operating concept of the Army of Tomorrow. See: http://fdts.kingston.mil.ca/DLCD-DCSFT/pubs/landops2021/Land_Ops_2021_eng.pdf.

dangerous.³⁸³ The successful introduction of robots on the battlefield has thus far been restricted to remote-controlled operating modes, due to a broad range of limiting factors.³⁸⁴ In other words, like most other tools, contemporary land-based robots generally require a full-time human operator if they are to be of any use. Although remote-controlled operating modes do contribute to overall mission effectiveness, even greater performance gains are anticipated as forthcoming advances in robot autonomy promise to liberate human operators from current one-to-one, direct full-time manipulation of the systems. In essence, land-based robots with greatly improved levels of autonomous intelligence³⁸⁵ and mobility will transition from being mere tools to being team members.

Humans use tools in order to enhance their natural abilities or to overcome their physical or cognitive limitations. For example, binoculars are used to augment human visual acuity and computers are used for performing complex numerical calculations in order to ease the cognitive burden, improve accuracy, and speed up the calculations. But in addition, when humans cannot successfully achieve their goals individually, even with the aid of tools, they form teams. Therefore, the robots that will offer the highest degree of military payoff for the Army in the future will be those that can be incorporated into human–robot, and robot–robot teams, where they work together to achieve common goals and missions while sharing responsibility and accountability for attaining results. In this way, future robots will decrease the additional physical and cognitive burden currently placed on soldiers for the operation of tele-robotic systems. As autonomous intelligence increases over time, robots will possess an ever better ability to react to their operating environment and demonstrate intelligent battlefield behaviours, where their degree of reaction will depend upon the sophistication of their artificial intelligence (AI), sensing, and mobility subsystems. That will offer the potential for robots to assume a greater portion of the tactical and operational burden and even to offload certain human burdens altogether. As intelligent robots begin to share responsibility for achieving objectives, they will no longer be mere tools: they will have to be regarded as team members. But before they can transition to team-member status, they will pass through an intermediate

383. In this context, tools are mechanical devices intended to make tasks easier; something to perform an operation; an instrument; a means.

384. These limitations include the ability to build environmental awareness, interpret commands, collaborate with other systems, operate in complex missions, operate autonomously—all of which are related to the capacity and strength of artificial intelligence. Other limitations that have to date prevented any sort of explosive robot growth in the LF include size and weight, power, mobility, survivability, communications (bandwidth, frequency management and interference), maintenance, interoperability, operational security, reliability, cost, and overall utility.

385. See <http://www.accelerating.org/articles/consideringsingularity.html>.

stage where they will be considered smart tools.³⁸⁶ To determine whether robots offer the most utility as tools, smart tools, or team members, an examination of both the cognitive and physical burdens typically faced by soldiers is required.

It will be paramount to keep in mind that the Army does not aspire to incorporate unmanned systems into its structure in the same manner as envisioned by the United States Army's Future Combat Systems project. The Army will pick and choose the niche areas where value can be maximized. Therefore, an analysis of the Army Task List will need to be conducted during future design work in order to determine where robots can be leveraged to work best.³⁸⁷ Large, costly robots are unlikely to be the best solution. Trends in other sectors indicate that small niche vehicles will surge in popularity, potentially indicating that the application of robots in the Army may be optimized in areas where a large number of inexpensive collaborative systems (versus large and expensive do-all systems) work best.

PART THREE – THE SOLDIER’S BURDEN

Typically we think of burden as physical in nature, but, for the purposes of this concept paper, burden must include both physical and cognitive soldier loads. Arguably, everything an individual does involves a degree of cognitive burden because all human actions manifest in the brain. The complexity of the environment and the problem at hand, together with the timeframe within which an appropriate response is needed, all contribute to the magnitude of the cognitive burden. Confusing choices, ambiguous situations, and situational complexity all add to the soldier's cognitive burden. Robots that conduct tasks associated with increased cognitive burden, such as those that involve choices and ambiguity, may help offload some of the human analytical overload (especially for those tasks well suited to numerical computation and simulation). Cognitive burdens are generally related to the Command and Sense operational functions. However, because they can never be separated from physical burden, they also relate to the other operational functions. The difficulty associated with performing any task must be measured on both the physical and psychological planes.

386. Smart tools may be equated to what is often described in the scientific literature as *semi-autonomy*. Smart functions may include auto-piloting, platform stabilization, and automatic frequency or sensor selection.

387. The Army Task List may be found on the DWAN at http://fdts.kingston.mil.ca/web_temp/DGLCD/15_AoT/BG%202021%20Study/Integrated%20Question%20List/Operational%20Function%20Task%20Lists.doc.

Physical burden exists largely under the operational functions of Sustain, Shield, Act, and Sense. The Sustain burden in this context concerns physical considerations related to the movement of personnel and materiel, as manifested in the processes of supply, resupply, maintenance, and CASEVAC. The Shield burden refers to weaknesses of the human body in its ability to endure physical effects such as shock, blast, or penetration. The physical Act burden relates to effects delivery systems and processes and encompasses the employment of weapons and influence activities. The physical Sense burden refers to the limitations of the human body's natural sensing capability, including visual, auditory, olfactory, and tactile sensing. Robots are capable of reducing all of these burdens or, alternatively, alleviating human limitations. Although potential robot applications are seemingly limitless, it is important to recognize that the Army will never have enough resources to do everything. It will be necessary to look at those tasks where automation might help, or those tasks in which the Army has a strong desire to improve performance, and prioritize where robots will likely have the greatest impact.³⁸⁸

Today's robots are primarily intended for offloading certain aspects of the soldier's physical burden. In that respect they are no different than any other tool in the military inventory.³⁸⁹ The tradeoff for soldiers for this reduction in physical burden is an increasing cognitive burden. For example, a robot used as a tool by EOD operators greatly decreases the risk of injury by offering better standoff, thereby reducing the overall physical burden on the soldier.³⁹⁰ However, the cognitive burden of the EOD operator increases.³⁹¹ The operator must not only still know how to disarm and dispose of the device, but also manipulate a remote-controlled robotic tool while doing so.

Robots will therefore result in the highest payoff for the Army when they are able to lessen one burden without contributing to increasing another. The process may be regarded as a transition from robots as tools to robots as team members. Robots have the potential to function as part of the all-arms team in each of the operational functions across the continuum of operations. A brief examination of each of those areas will highlight the desired vision for robot capability. Note that the Command operational function will not be discussed, as burden reduction in this function is consistent with the use of

388. Again, this underscores the requirement for an analysis of the Army Task List.

389. Because robots are considered another tool, some authors argue that conceptual work leading to doctrine for robot employment in land operations is not required. For example, see page 19 of the US Army *Robotics Strategy White Paper*.

390. The physical burden relates to the potential for traumatic blast injuries. Physical burden in this sense may be equated with risk.

391. Admittedly, because of the reduction of physical risk, some of the operator's cognitive burden is also lowered because the consequence of error is greatly reduced.

the aforementioned agents or bots. Physical ro-bots have little utility within this operational function, save for their ability to contribute to a reduction in complexity and decision making.

PART FOUR – ROBOTS AND THE OPERATIONAL FUNCTIONS

Within the Sense function, robots currently offer a significant contribution to military operations. Overwhelmingly, however, these robots operate within the air environment. The physical ground environment has thus far proven too great a challenge for the employment of robots in any sort of sensing role beyond limited local collection at the lowest tactical levels.³⁹² To determine how robots can best contribute, we must identify where humans have the most difficulty. For example, unmanned aerial vehicles (UAVs) have surged in popularity because of their ability to easily overcome human field-of-view and line-of-sight range limitations. That capability has reduced the overall cognitive burden associated with building a mental picture of the environment and the physical burden associated with manoeuvring ground forces in order to get a better look at an objective area.³⁹³ A ground-based robot must offer a similar tradeoff.

The Army ISTAR system describes the group of activities related to the Sense operational function. Even with the proliferation of sensor feeds from UAVs, there are still deficiencies in the ability of the Army to execute the ISTAR process. Those shortcomings can be offset by the use of ground-based robots. Technology is sufficiently advanced today to permit ground-based robots to conduct certain short-range ISR missions.³⁹⁴ The Dragon Runner™ platform currently in service with the Army provides the soldier with enhanced improvised explosive device (IED) detection ability and an urban reconnaissance capability. UAVs are limited in their ability to see inside structures, but robots like Dragon Runner™ are not. This first generation of lightweight urban ground reconnaissance robots is integral to section-level manoeuvre and offers useful, though limited, enhancement of the immediate

392. However, information-gathering robots are gaining momentum. The US currently uses more than 12,000 ground-based robots in its operations in Iraq and Afghanistan, many of which have an ISR role and are therefore contributing to better situational awareness at the local level. Infantry sections, for example, have already reaped the value of live full-motion video taken inside urban structures by portable remote-controlled robots. However, the intelligence community has yet to benefit from these urban robot sensor feeds, owing to the fact that robots do not upload their feeds to the network. That denies intelligence forces the ability to build more detailed databases and knowledge repositories.

393. UAV feeds add their own cognitive burden in the form of information overload. However, too much information is better than not enough. This observation confirms the requirement for better analytical tools and information-management procedures, both of which may be improved in the future by stronger AI and computing algorithms.

394. Throwbot™, Bombot™, and Dragon Runner™ are modern examples of robots employed in the conduct of ISR missions.

ISTAR capability of the section. Future generations of Army sensing robots will offer significant operational advantages by being able to reconnoitre independently. Such advances will allow these robots to autonomously build images and maps of urban structures and relay the images to higher headquarters via tactical networking. These robots will also have the ability to discern relevant information pertaining to priority intelligence requirements and conduct real-time autonomous tracking of objects of interest. In this respect, robots will assist with the generation and dissemination of intelligence information through autonomous reconnaissance activities. Control of the robot and other information exchange will evolve from present-day remote-controlled operation by dedicated operators and controller systems to network-enabled command and control (semi-autonomy) and, in some cases, to full autonomy in a mission-command environment where robots infer their tasks based on knowledge of the commander's intent.

Robots will also be incorporated into the Shield function. Today's robots provide standoff in the conduct of tasks involving dangerous environmental situations. CBRN and explosive (CBRNE) detection and defeat are representative of tasks where ground-based robots have already seen a measure of success in testing and on operations.³⁹⁵ In general, contemporary robots rely upon a dedicated operator and a wired control station for real-time remote control. Although wireless solutions exist, problems with communications and signal processing greatly limit the standoff range granted to the operator. Nevertheless, providing any amount of standoff distance through the use of remote-controlled robots in dangerous environments generates an immediate casualty reduction benefit. For some tasks, such as minefield clearance, robots will be able to work at a faster than human pace, because clearance robots' mistakes do not generate human casualties. The cost of Shield function-related robots, however, must be kept as low as possible because they are likely to be rendered inoperable while in service.

Future robots will form part of the omni-dimensional shield, a concept encompassing protection of soldiers, partners, non-combatants, platforms, systems, equipment, and facilities from such threats as CBRN, aerial, psychological, direct kinetic, and unintended friendly fire (fratricide). Whereas robots employed in today's counter-IED fight require a dedicated operator with a dedicated control unit, future systems will traverse routes

395. Some examples include the Improved Landmine Detection System (ILDS), Doking MV4™, the Multi-Agent Tactical Sentry (MATS), and Talon/Packbot™ CBRN.

autonomously—in accordance with mission directives pushed through the network from controllers at higher headquarters—locating and neutralizing explosives threats on their own, while constantly feeding the network with information related to their activities.³⁹⁶

Within the Act operational function, current robots are capable of delivering a range of weapons effects to the enemy.³⁹⁷ Lethal combat engagement is the most controversial robot application, because it is not well defined within the law of armed conflict (LOAC). Today's systems operate in human-in-the-loop (HITL) mode only.³⁹⁸ Although the Army has maintained robots that can be used as remote weapon systems within its inventory for more than thirty years, they continue to be employed only for ballistic breaching tasks and not in an anti-personnel role. Although the incorporation of lethal robots into the Army arsenal is highly desirable because they offer a faster sensor-to-shooter link with considerable standoff advantage due to their non-line-of-sight (NLOS) operation, it will remain imperative that such systems stay under HITL control. Despite ongoing R&D activities across the globe to the contrary, only HITL operations can ensure compliance with the LOAC.³⁹⁹

The Achilles heel of Army expeditionary operations has traditionally been logistics. Therefore, robots that can maximize logistical efficiency or advantage will be essential to the conduct of future operations. The Sustain operational function will be greatly enhanced by the employment of robots that offer the ability to optimize combat service support operations while at the same time protecting soldiers from exposure to combat engagement.

The echelon system is well suited to the use of multiple layers of robotic systems, although current robots operating within the Sustain function are not yet able to meet all the necessary requirements for expeditionary operations. Improvements in the areas of OPSEC, mobility, maintenance, and power will be needed to ameliorate this situation. In the future, robots will move materiel from point to point using technologies such as robotic mules at section level, unmanned logistic vehicles at sub-unit level, and autonomous convoy systems

396. The Guardium™, MDARS™, and SGR-A1™ are examples of existing robots with autonomous movement and detection capabilities. They are, however, best suited to static, low-threat environments.

397. Some examples of robots developed for fire support include the BAE Black Knight™, MAARS™, Gladiator™, and Switchblade™. Robots designed for assault breaching include the Pearson Assault Breacher Vehicle™ and CMU Crusher™.

398. In other words, they have dedicated operators and control equipment and can fire upon a target only when a human confirms the targeting information and physically instructs the robot to engage.

399. There is a grey area worth mentioning: a time lag between when the HITL authorizes an engagement and when the robot actually fires. Depending on how long the lag is, there may be a requirement for certain degrees of autonomous operation for such robot shooters in order to ensure that the rules of engagement and the LOAC are properly applied.

at unit level.⁴⁰⁰ However, research and development activities do not have to focus on building wholly new robotic vehicles. Existing technologies that can be automated with relative ease (thereby delivering the same capability at lower cost) must be exploited to the fullest. The Army need not invest in new kit if it can build more intelligence into the tools it already has.

PART FIVE – INTEGRATING THE ROBOT TEAM MEMBER

There is no requirement for an overarching robot concept for robots that are employed solely as remotely operated tools. Thus there is currently no doctrine guiding the employment of unmanned systems. Yet the need for such doctrine will increase in proportion to the increase in capability, utility, and presence of unmanned systems on the battlefield.⁴⁰¹ Considering that capability will be directly proportional to the sophistication of AI governing system behaviour, and that AI is becoming ever more advanced, it is expected that robots will be able to function as team members in certain roles as early as 2020.⁴⁰² Now is therefore the right time to begin developing principles for their integration as full-fledged members of the all-arms team, because once robots transition beyond being mere tools, they hold the potential to revolutionize the way in which operations are conducted.

Several methods of incorporating robot team members have already been described. They range from fully autonomous operations within the ISTAR system to autonomous movers armed with remote-controlled weapon systems. Thus, the transition from tools to team members may be regarded as a shift from robots controlled by dedicated operators to distributed autonomous systems operating within the spirit of mission command while intermittently controlled by inputs from intelligent agents residing on the network itself. Numerous barriers need to be overcome before robots can be successfully transitioned from tools to team members. In addition to the technological limiters already described, certain institutional barriers must also be overcome. They include the pace of procurement, resource constraints, legal ambiguities, and the impact of automation on military culture and tactical standard operating procedures. The best way to overcome those barriers is to continue introducing robot tools into field units. That will allow units to become

400. The appeal of unmanned logistical convoys is largely related to minimizing exposure of logistics forces. Whether or not this reduces the convoy force protection requirement must be the subject of future analysis.

401. Samuel N. Deputy, *Counterinsurgency and Robots: Will the Means Undermine the Ends?* Paper submitted to the Faculty of the Naval War College, Newport RI, 04 May 2009. DTIC. 29 July 2010: <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA503005>. 2-5.

402. Robots capable of operating in fully autonomous modes are not expected within the next 10 to 15 years.

socialized to the use of robot tools and help soldiers recognize the potential utility of the tools as team members.⁴⁰³ It is therefore imperative that the introduction of robotic systems relieve some of the burden on an already overburdened force. If a robot adds to operational complexity without delivering sufficient benefit, it will most certainly be discarded by its operator, and any such rejection risks introducing a secondary effect of loss of operator trust in robotic systems. Therefore, robot tools must be easy to operate, with common user-friendly human-robot interfaces. Co-opting the interfaces from popular commercial gaming systems will likely offer immediate practical benefit, but the ideal interface will likely be one that accommodates natural language and gesture interaction between human and robot. Simply put, less time spent learning the operation of the tool leaves more time to spend on developing creative uses for that tool.

The next stage of the introduction of robotic systems into the Army—the shift from robot tools to autonomous systems—cannot occur without supporting network developments. Robot team members, therefore, cannot be introduced to units until an adequate network infrastructure is established. Implementation of the future network concept and the robot team concept are both heavily underpinned by technological developments and therefore must proceed in lockstep. Notwithstanding this interdependence, long-heralded advances in artificial intelligence capabilities are also a necessary condition for this transition.

In terms of potential future tasks for robots in land operations, it is unlikely that fully autonomous systems will be suitable or desirable in all situations. In other words, only a portion of all robot tools will need to transition into the role of robot team members. The desirable level of autonomous operation for each robot in the force must therefore be clearly analyzed prior to capability development activities in this area. The primary motivation for introducing robot autonomy is the need to relieve the cognitive burden that humans face in the increasingly complex and time-constrained operating environments in which they operate. In other words, the more decisions that robots can make independently within a mission command context, the more time humans will have available to focus on decision making that requires human-level judgement and understanding.

403. Defence R&D Canada's Technology Demonstration Program (TDP) is perhaps the optimal method to control the gradual but continuous incorporation of robots into the LF. See <http://www.drdc-rddc.gc.ca/sciences/tdp-pdt-eng.asp>.

PART SIX – MODULARITY: AN ESSENTIAL CONSIDERATION

To help describe what is meant by modularity, it may be useful to borrow satellite systems nomenclature. Robots include three primary components: bus, payload, and subsystems. The bus includes all components that ensure locomotion, i.e., the movement of the robot from point to point. It may also be regarded as the unmanned vehicle or platform component. The payload refers to all instruments on board the robot that carry out the actual robot mission. Lastly, subsystems include any components designed to support the payload or the bus. Robot subsystems might include power, temperature control, navigation, protection, and communications. Modular systems will seek economies in bus and subsystem design while maintaining the ability to incorporate multiple payloads on any given bus.

PART SEVEN – OTHER DESIGN PRINCIPLES

In addition to modularity, there are other design principles that must be adhered to in the development of future robot systems. They include autonomy, interoperability, and resistance to tampering. Each of those principles will ensure that commanders have the highest possible degree of flexibility in incorporating robots into their operations. Though many tasks are conducive to full automation, there are some tasks for which robots must remain tools and not full-fledged members of the all-arms team. Roles in which robots are more desirable as tools than as team members may include casualty care and direct or indirect fire support.

The degree of desirable robot autonomy will be situation- and task-dependent. Higher degrees of autonomous operation decrease the human cognitive burden because robots are programmed with their own tactical and cooperative behaviours (e.g., swarming). Some robots will also have the ability to learn appropriate responses and behaviours. It should be noted that it is not always desirable to have robots that can learn and adapt. The nature of the robot mission will be the determining factor in whether adaptation and learning will be considered a desirable feature. Robots will operate across the continuum of operations, and a lesson learned in one context is not necessarily applicable to other situations. Learning behaviour is therefore best instilled in robots used in contexts where mission success will not be put at risk if a robot learns a sub-optimal (or wrong) lesson. The desirable degree of robot autonomy will also be the defining characteristic of whether or not a robot tool or a robot team member is required for a given task. There will be times

when limited autonomy, or a smart tool, is all that is required. In other words, we automate as much as we need to and no more.



Source: Combat Camera

PART EIGHT – GRAPHICAL MODEL OF THE HUMAN-ROBOT TEAM

Presented below are two models for the employment of robots on operations. The first depicts the human-robot relationship of today; the second shows a more futuristic vision of the human-robot team.

In the model presented above, humans are involved only in steps 3, 4, and 5. Robots are involved in steps 2 and 6. In the case of an EOD robot, 2 and 6 are the same robot, while 3, 4, and 5 are the same human. In the case of a Predator UAV, 2 and 6 are the same robot, but 3, 4, and 5 are not the same humans. Different concepts for the use of robot tools can integrate or separate the platforms in steps 2 and 6. Likewise, 3, 4, and 5 can be one human or many distinct teams of humans.

The blue text in Figure 3.8.2 shows the differences between it and Figure 3.8.1, which depicted robots as tools. In Figure 3.8.2, robots are no longer confined to steps 2 and 6. Robots have more roles and responsibilities in steps 2 and 3.

The robot also has the potential to replace and/or augment humans in steps 4 and 5. Different combinations of robots and humans are now possible throughout the cycle.

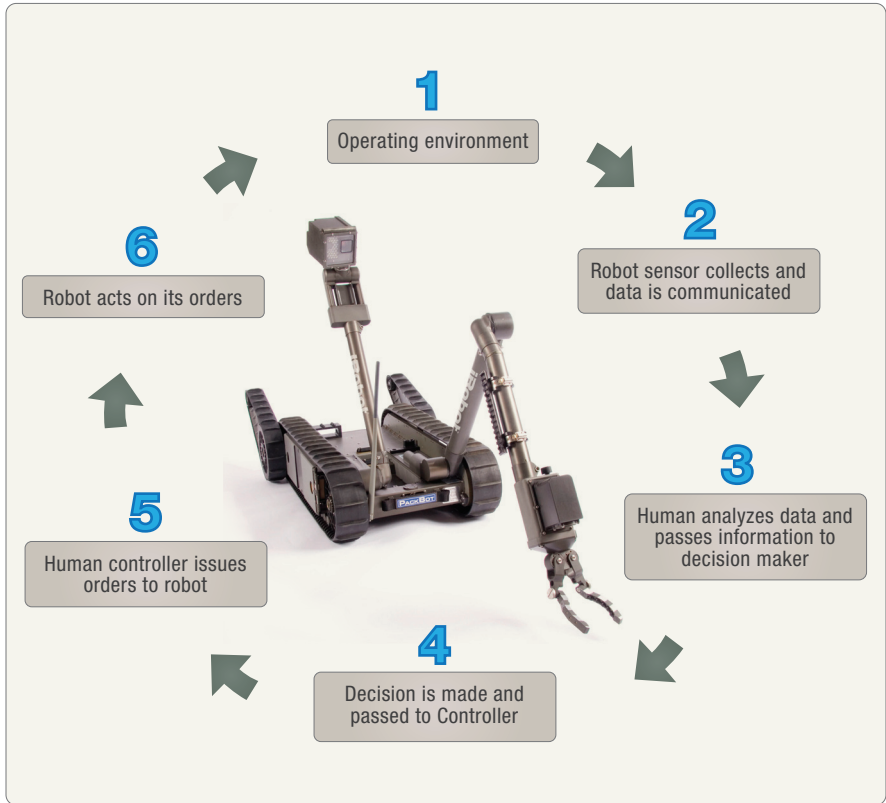


Figure 3.8.1: The Present: Robots as tools

We need to stop thinking of an autonomous system as just one robot capable of following all the steps by itself with no need for human input/collaboration. We often mistakenly equate autonomy with steps 4 and 5, but really autonomy refers to the ability to carry out step 3. Even then, the robot may be augmented by human teammates in carrying out that step. Remember, even humans are not necessarily free to carry out steps 4 and 5 in all situations; that is why humans must work in teams or units.

The blue text also indicates areas where further research and development work is needed.

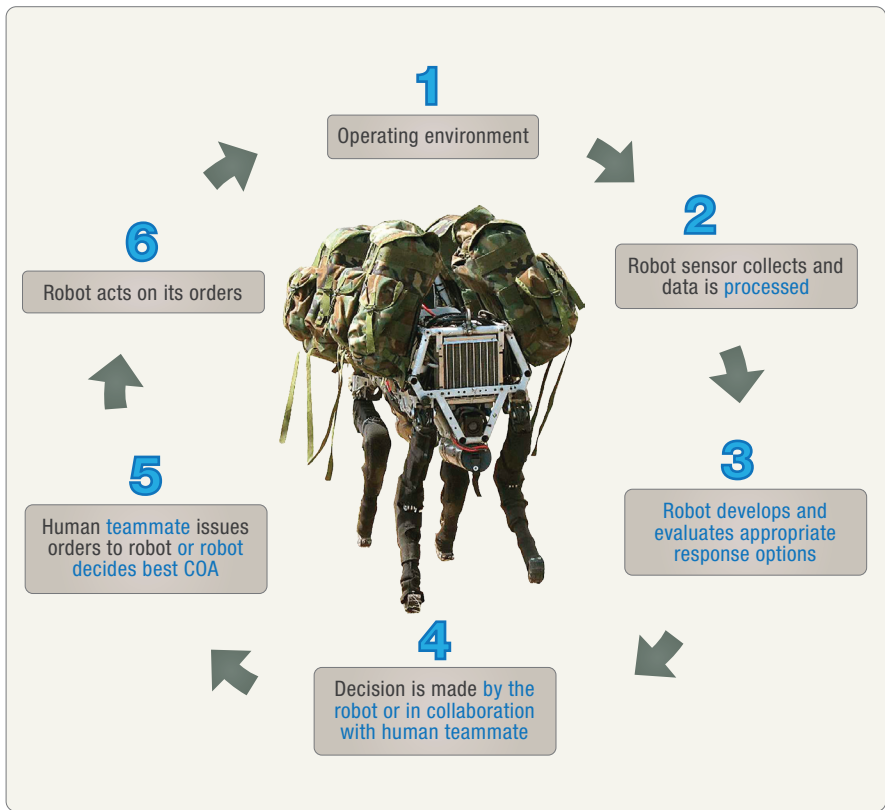


Figure 3.8.2 : The Future: Robots as Team Members

PART NINE – UNMANNED SYSTEMS TAXONOMY

As an update to the framework described in Part Eight of the previous chapter, DLCD presented an unmanned systems taxonomy to the Army Capability Development Board in June 2011. The taxonomy puts a finer point on some of the terminology associated with unmanned systems and helps delineate differences between the seemingly interchangeable terms in the domain.

The taxonomies put forward in this book are not meant to be enduring. Rather, they ought to be used to guide future discussions with joint force development organizations and the warfare centres resident in the other services, in order to reach consensus on a universally accepted CAF taxonomy.

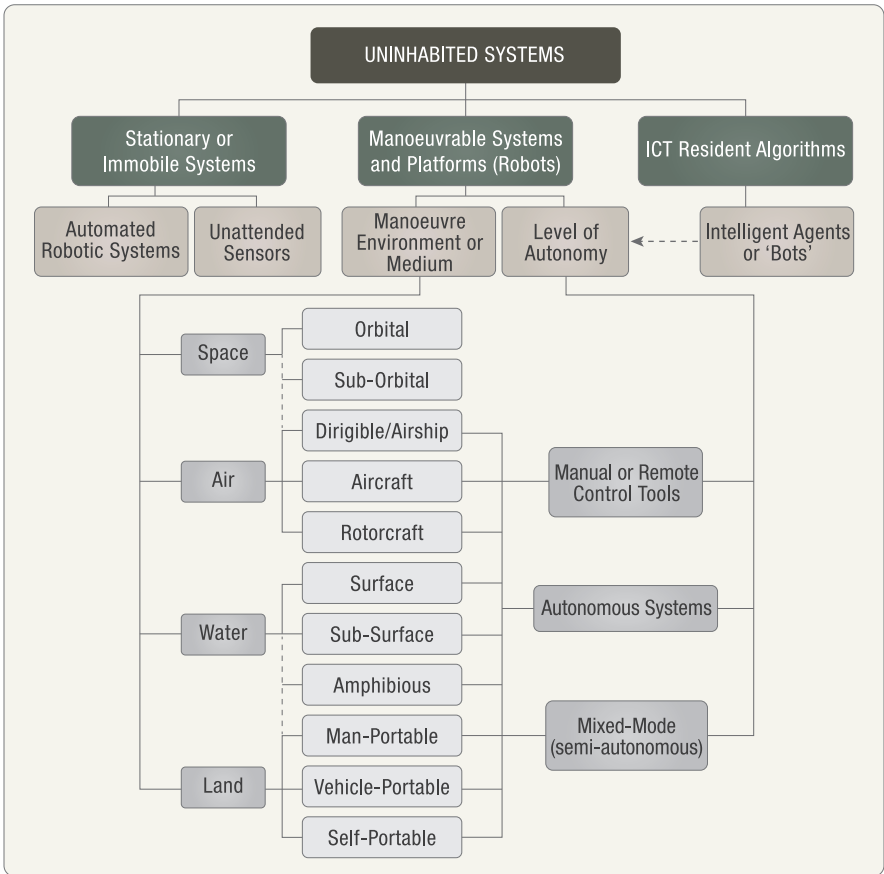



Figure 3.9.1: Unmanned Systems Framework

PART TEN – CONCLUSION

Robots are beginning to contribute significantly to the conduct of land operations. Beyond the great successes associated with UAV integration, ground-based remote-controlled systems are also gradually becoming more prominent. As technological limitations are overcome by the R&D community, the utility of terrestrial robots will extend beyond their use as mere tools. Robots will become increasingly smart and eventually become integral members of the Army team as they become more capable of sharing the physical and cognitive burden with their human counterparts. The potential they hold to revolutionize land operations demands that their incorporation into the force continue. Although budgetary constraints may tempt capability



developers to temporarily sideline investment in robots, the most sensible way forward may be found in incremental builds that capitalize on the successes and learn from the failures of previous robot iterations.⁴⁰⁴

404. Author's note: This chapter is based largely on a concept paper written for DLCD which included significant contributions from Regan Reshke, Scientific Advisor to Chief of Land Strategy, and Lieutenant Colonel (AUS) Brendan Dwyer, the Australian standardization representative to the Canadian Army.

CHAPTER 4

FUTURE CONCEPT FOR ARMY USE OF SPACE- DERIVED CAPABILITIES



Source: Wikimedia NASA

“Our dependency on space-based capabilities is such that the CF must now assess its ability to achieve operational success in theatres where access to space capabilities could be denied, disrupted or severely limited.”

—National Defence Space Strategy (draft 2010)



Source: Combat Camera

PART ONE – INTRODUCTION

The Canadian Army (CA) has become dependent on capabilities currently derived from space-based systems. Whereas space-derived capabilities were once considered a force multiplier, they have now become essential to the successful conduct of land operations. This dependence will arguably increase over time, especially in light of the CA future force employment concept of adaptive dispersed operations (ADO). Space provides a medium for the CA to achieve information and decision-making dominance over the adversary and across the continuum of operations. That means that it must be exploited as much and as thoroughly as possible. Increased reliance on space, however, is directly proportional to increased vulnerability. It is therefore imperative that the Army consider which space systems are essential for the conduct of its future operations and develop a multi-domain solution in case essential space assets are rendered inoperable.



Source: Combat Camera

PART TWO – SPACE OPERATIONS BACKGROUND

The space environment is one of five components of the physical plane; the others are land, air, maritime, and the electromagnetic (EM) battlespace. Much like the EM battlespace, space is not the sole purview of one environmental commander. Its global nature lends itself to influence over land, air, maritime, and cyber operations alike. Because it is regarded as the so-called ultimate high ground, and because it is part of the global commons, it is key terrain—or even vital ground for some operations—that cannot be seized, but instead must be shared. Being forced to share space with the adversary is not a comfortable position for military forces.

Space operations include four distinct mission areas:

- space support;

- space control;
- space force application; and
- space force enhancement.

2.1 SPACE SUPPORT

Space support includes spacecraft operations, such as space-lift and satellite operations (i.e., telemetry, tracking, and commanding (TT&C) and rendezvous or proximity operations).⁴⁰⁵ Although space support is not traditionally regarded as an Army mission area, any future concept that envisions the CAF with integral launch capability must consider space support, including satellite operations, as an essential component.

2.2 SPACE CONTROL

Space control includes the following functions:

- **Offensive Space Control.** This encompasses actions taken to deny the adversary's space forces freedom of action. Offensive space control consists of two processes:
 - ▶ **Prevention.** These are actions taken to prevent the hostile use of friendly or third-party space systems. For example, denial of GPS signal or RADARSAT II imagery to an adversary would be considered prevention. Prevention operations might also include the use of other instruments of national power such as diplomacy and economic sanctions.
 - ▶ **Negation.** Active and offensive measures taken against an adversary's space systems are collectively termed "negation."⁴⁰⁶ The five Ds of negation are deception, disruption, denial, degradation, and destruction.

405. Satellites are controlled through TT&C. Some TT&C is required for all satellites, regardless of the payload they carry. *Uplink* is data sent from the ground to the satellite; *downlink* is data sent from the satellite to the ground. Those links are used to receive *telemetry* data from the satellite and send command *data* to the satellite.

406. The four segments of any space system include the ground segment (command and control facilities), the space segment (orbital spacecraft and their payloads), the data communications link (the actual electromagnetic signal and the information it contains), and the user segment (including forces and equipment). Negation, therefore, is not synonymous with the weaponization of space.

- **Defensive Space Control (Protection).** Defensive Space Control includes active and passive actions to defeat adversary negation attempts and includes tasks such as detect, characterize, attribute, and defeat. Defensive measures will depend on the actual segment being defended. They include the following:
 - ▶ **Ground Segment Protection.** Protection measures here include security, the use of covert facilities, camouflage, concealment, deception, mobility, and hardening.



- ▶ **Space Segment and Link Protection.** Measures of protection here include establishing alternate nodes and employing radiation hardening, advanced signal monitoring, protection from space debris, adaptable wave forms, spare satellites, link encryption, and strong signals. Space and Link segments are grouped together because they employ several common protection mechanisms.
- **Space Situational Awareness (SSA).** This includes surveillance of space (SofS) capabilities—regardless of whether sensors are actually located in space or elsewhere—required for the development of a space common operational picture (SCOP). The SCOP includes space weather data, information on objects moving through the space area of interest, and orbital information for satellites and orbital debris. The monitoring of space enables protection and deters attacks. Although the Army does

not require an integral SofS capability, it could greatly benefit from having a SCOP coupled with access to timely and meaningful analysis.⁴⁰⁷

2.3 SPACE FORCE APPLICATION

The third space mission area is space force application. It is defined as “combat operations in, through, and from space to influence the course and outcome of conflict by holding terrestrial targets at risk.”⁴⁰⁸ The use of space-derived capabilities for the direct application of force against ground-based targets holds great potential for the conduct of future land operations. It should be noted, however, that Canada does not support the basing of weapons in space for the purpose of terrestrial or space attack (this policy point will be discussed in greater detail further on). In addition, the cost of such weapons may prohibit their development for the next several decades.

2.4 SPACE FORCE ENHANCEMENT

Space force enhancement includes five functions:

2.4.1 SATELLITE COMMUNICATIONS (SATCOM)

SATCOM enables the Army to maintain command and control over highly dispersed forces across large geographic distances. It includes all communication devices that exploit space-based assets: not only rear link systems that connect computer, telephone, and video teleconferencing networks between Canada and deployed locations, but also tactical communications such as radio (like the AN/PRC-117F and the AN/PRC-148 multi-band radio sets); telephone (such as Iridium and INMARSAT technologies); and tactical computer networks that include tactical satellite links which connect command and control computer systems between formation and unit headquarters and, when required, down to forward deployed sub-units and sub-sub-units.⁴⁰⁹

407. For example, knowing when adversarial/commercial/foreign imaging satellites are overhead, or knowing when the optimal (or suboptimal) GPS configurations occur. Knowledge of satellite geometry is important because it directly relates to GPS accuracy, which in turn has a direct impact on precision strike capabilities—a phenomenon known as “dilution of precision.” These factors, obtained only through SofS, may be critical to the staff’s ability to synchronize operations and avoid undesirable effects.

408. This definition was provided by the Advanced Space Operations School in Colorado Springs, Colorado, USA.

409. These systems include those presently fielded by the CA, or in various stages of development, such as the Tactical Satellite Kit (TSK) and the Tactical Satellite Link (TSL) in its three configurations: Heavy-TSL(H), for static deployed areas; Mini-TSL(M), for mobile locations; and on-the-move-TSL(OTM), for vehicular usage.



Source: Wikipedia

2.4.2 POSITIONING, NAVIGATION, AND TIMING (PNT)

PNT is another essential space-derived capability that enables land operations. Positioning and navigation are made possible by the Global Positioning System (GPS) and are best represented by the GPS user segment, which includes hand-held devices such as the Precision Lightweight GPS Receiver (PLGR) and the Defence Advanced GPS Receiver (DAGR).⁴¹⁰ The use of GPS has enhanced the

410. The primary mission of the GPS is to provide precise, all-weather, three-dimensional position, velocity, and time (PVT) information to an unlimited number of properly equipped military and civilian users across all physical environments. GPS information is real-time, passive, and referenced to a common grid position. GPS supports military forces in peacetime and in the conduct of wartime operations. GPS wartime navigation support applications include en route navigation, low-level navigation, target acquisition, close air support, missile guidance, command and control, all-weather air drop, sensor emplacement, precision survey, instrument approach, rendezvous, coordinate bombing, unmanned aerial vehicle (UAV) operations, search and rescue, reconnaissance, range instrumentation, and mine emplacement.

Army's ability to navigate across featureless expanses and through crowded built-up areas alike with relative ease, while at the same time providing it with a system that can ensure precise friendly force positioning information. Though the Army's initial iteration of friendly force tracking or blue force positional awareness (via the Situational Awareness System) has had mixed results, that will change in the future when commanders have access to more reliable and more automated systems giving them precise knowledge of where all friendly forces are deployed. Military exploitation of the PNT component has also enhanced the Army's ability to do precise targeting using precision-guided munitions. It has also allowed the Army to develop highly accurate terrain and mapping tools via other systems such as satellite imagers and manned and unmanned air platforms.

- **Time Transfer.** Time transfer has become the most commonly used application of GPS. Not only is GPS timing used for digital communications and as time hacks for bombs on target, but in addition the commercial world is using it extensively in the banking community and to synch up networks, including the Internet itself. Time transfer from the GPS constellation is responsible, in large part, for all computer network synchronization. Without it, simply put, the networks would not work. Extended loss of GPS signal would eventually result in the inability to prosecute computer network operations (CNO).⁴¹¹

2.4.3 **SATELLITE-DERIVED INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR)**

The ability to obtain persistent overhead imagery of terrain, infrastructure, equipment, and personnel ensures the Army's ability to see first, understand first, decide first, and act first; i.e., its ability to dominate across the continuum of operations. Satellites not only provide detailed multi-spectral⁴¹² images of a commander's area of operations and area of interest from orbit, they also act as the communications backbone that allows for the operation of unmanned aerial vehicles (UAVs) that provide the Army with more detailed imagery and full-motion video. The signals intelligence (SIGINT) function is also reliant on certain space-derived capabilities.

411. Computer networks have other methods available to them to effect clock synchronization, but GPS is fast becoming the standard time-transfer system. Internal clocks can keep time on their own, independent of a master clock, for anywhere between a few hours and a few weeks.

412. Multi-spectral imaging (MSI) includes data captured from the same source in different electromagnetic spectral bands. There are four different types of MSI resolution: radiometric (a function of relative brightness), temporal (depends on revisit rates), spatial (the smallest distance between two objects at which the objects appear separate and distinct), and spectral resolution itself, which includes multi-, hyper-, and ultra-spectral imaging, each with a progressively higher degree of discrimination between spectral bands.



2.4.4 ENVIRONMENTAL SENSING

The nature of military operations and the difficulties associated with obtaining reliable terrestrial-based weather and terrain information in foreign countries dictates a requirement for space-derived capabilities. Environmental sensing includes the following:

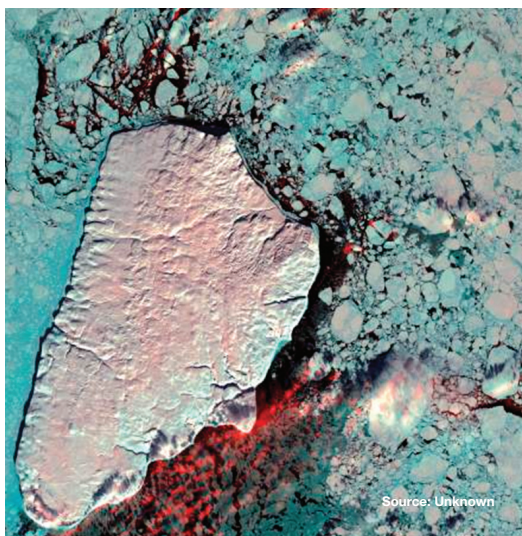
- **Atmospheric Weather Monitoring.** Weather must be considered in terms of its influence on mobility (trafficability and route selection), visibility, air support, munitions selection, targeting, battle damage assessment, troops and equipment, and the effects of chemical, biological, radiological, and nuclear (CBRN) weapons.
- **Space Weather Monitoring.** The inhospitable operating environment of space can significantly degrade all space-based capabilities. Objects in

space are subject to combinations of the most dangerous environmental conditions imaginable.⁴¹³ The Army requires situational awareness on each of these space weather phenomena insofar as they impact on any of its space-derived enabling capabilities.

- **Terrain and Hydrographic Monitoring.** This function is largely centred on the generation of geomatics data and information needed for mapping and the development of mapping tools, map models, and geo-intelligence.

2.4.5 MISSILE WARNING

Any self-propelled guided weapon system launched from or through space can only be tracked using space-based sensors. These missile warning satellites are used to cue missile defence systems (ground- or air-based) to protect ground forces from tactical ballistic missile attack. Space-based theatre missile warning is conducted using assets already in place which provide the nuclear early-warning umbrella. Such assets are operational 24/7 with global coverage by nuclear nations that possess an Intercontinental Ballistic Missile (ICBM) capability. Global missile warning coverage is driven by the need to avoid a mutually assured destruction (MAD) scenario.



413. Those conditions include extreme heat, extreme cold, plasma (causing arcing, unstable electrical currents, ion drag, and ion sputtering), radiation (including elementary and nuclear particles—both charged and electromagnetically neutral—from the sun and the Earth's Van Allen belts, causing degradation of solar cells, electronics, and materials as well as single-event phenomena and fluctuating solar radiation pressure), micro-meteoroids and orbital debris, extreme velocity, vacuum environment (causing out-gassing, ultra-violet degradation, cold welding, and thermal control problems), neutral atmospheric conditions (resulting in atomic oxygen attack, physical sputtering, and spacecraft glow), extreme variations in aerodynamic drag (caused by expanding and contracting atmospheric layers), and scintillation.

PART THREE – CAPABILITY DEFICIENCY: ASSURED ACCESS TO SPACE FORCE ENHANCEMENT

The four space mission areas described above include a host of capabilities that the CA does not currently possess. To date, CA space operations capability has largely been within the space force enhancement mission area. Because the CA does not possess a space support capability, it cannot have assured access to Space Force Enhancement or Space Control functions on its own. If neither the CAF nor the Government of Canada has the ability to conduct space support, then there can be no assured access to any space-derived capabilities for the CA.



3.1 POTENTIAL OPTIONS

Access to space-derived capabilities must therefore be achieved through any, or a combination, of the following means:

- **Partnerships.** These would include civil, commercial, and international (including international military) agreements or cooperative ventures.

- **Integral Launch.** This implies the development and employment of a Canadian-based capability—the only true means of assured access.
- **Multi-Domain Solution.** This would see redundant systems (in space and across multiple environments) that deliver similar force enhancement capabilities which are currently associated primarily with space-based systems.

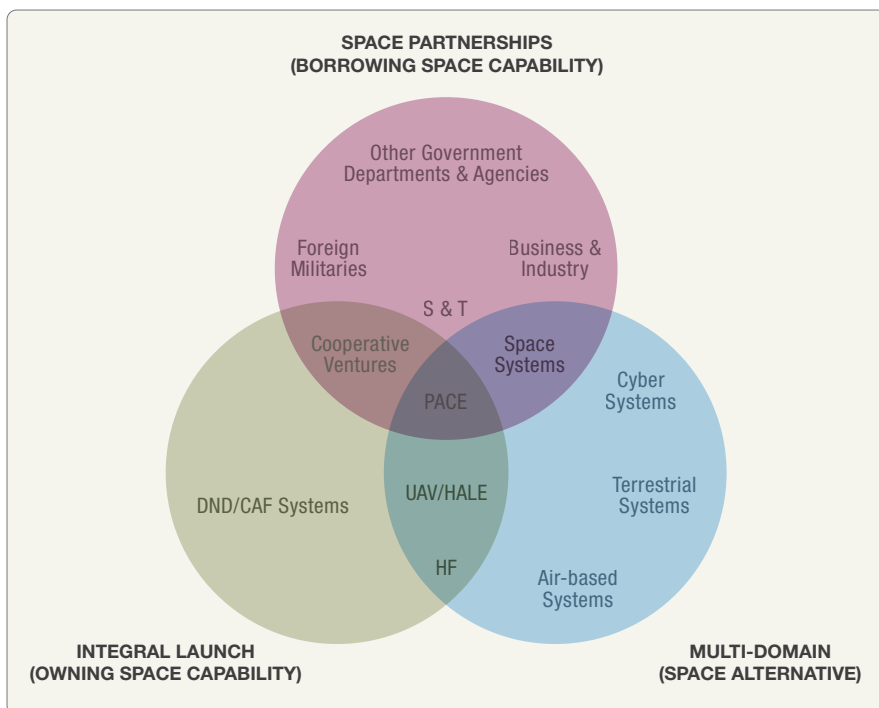


Figure 4.3.1: Potential Space Options

The draft *National Defence Space Policy* states that assured access to space-derived capabilities underpins the future of Canadian military operations (including land operations). This indicates that an alternative to space-derived capabilities has not been incorporated into joint doctrine; if there was an alternative, then access to space would be a “nice-to-have” capability rather than a “must-have” capability. The danger of incorporating assured access into doctrine is that it implies an inability to prosecute military operations without such access. Moreover, such a policy would surely be extremely costly in the near term, since Space Support and Space Control infrastructure and technologies do not come cheap, at least not today.

3.1.1 PARTNERSHIPS

Because the CA does not have the capacity to control space, it is wholly dependent on its joint, interagency, multinational, and public (JIMP) partners to provide it with the space force enhancement capability it needs to operate. Developing partnerships represents the optimal way to gain from space force enhancement functions while incurring minimal R&D effort and financial expense. Partnerships, however, also come with a degree of risk. Canadian Forces reliance on commercial or civil partners for space support and space control functions leaves the military potentially vulnerable to economic circumstances and competing interests. This risk also extends to CAF dependence on the military space systems of other nations. CAF space force enhancement capability could be significantly degraded depending on future military, economic, or diplomatic circumstances. Such risk can be mitigated through the development of multiple partnerships, thereby assuring the CAF's ability to access space force enhancement functions from redundant sources. Rather than simply focusing on economic partnerships, it could also explore promising technological partnerships. For example, focusing the national R&D effort on technologies of interest to our partners has the added benefit of forcing them into technical dependence. That would enable Canada to become an actual contributor to those systems that the CAF relies upon, thus minimizing the risk of losing access.⁴¹⁴

3.1.2 INTEGRAL LAUNCH

Integral launch capability remains expensive. The cost may be lessened with cheaper future technologies. Although the establishment of a land-based launch facility within Canada may be highly unsuitable owing to the incredible expense, the inability to gain operational responsiveness, and geography, the defence R&D community and its partners ought to explore other potential launch techniques and technologies.

Potential Space Support technologies that may be more attractive in the future may include air- or sea-launch platforms which offer the CAF a more operationally responsive capability unconstrained by geography. Such technologies would need to be supported by even more systems, such as simpler (more automated), cheaper, and more easily portable ground-control

414. This assumes an existing partnership between DND and other Government of Canada (GoC) departments, agencies, and relevant Crown corporations. Partnerships must be extended from this GoC grouping to also include Canadian and international business concerns and military partners.



Source: Wikipedia

and tracking stations.⁴¹⁵ The simplest solution may involve launching satellites into geosynchronous orbit (GEO), thereby minimizing the Space Support requirement. That is still no easy task, however, as it requires a great deal

415. If integral launch is being considered as an option, Canada must maintain the capability to conduct Space Support satellite operations throughout the spacecraft's orbit. That means either developing a network of terrestrial control or receiver stations (which is expensive), partnering with nations that already have such a network in place, or harnessing the crosslink (satellite-to-satellite) communications capability of other satellites.

more energy to place a satellite in GEO than in low-earth orbit (LEO). Furthermore, satellites in GEO are great for communications, but poor at conducting ISR tasks. Small satellite technology may be another solution (it will be further discussed below). In short, integral launch is the essential component of the doctrine of assured access. Assured access, however, may not be required if sufficient partnerships are developed and backed by a multi-domain solution.

3.1.3 MULTI-DOMAIN

The multi-domain option refers to any effort aimed at creating redundancy in space and in the other environments aimed at providing multiple means of acquiring the products and capabilities of space force enhancement functions. The risk and expense associated with this solution uncertain. Therefore, the multi-domain option must be further developed through a process of simulation, experimentation and operational research to determine the optimal mix of land-, air-, and space-based capabilities.

3.2 VULNERABILITIES

Space-based systems are characterized by a high degree of vulnerability because of two primary factors:

- the extreme physical environment (as described above); and
- the potential weaponization of space.

Canada is a party to the Outer Space Treaty, which prevents its involvement in any activities related to the weaponization of space.⁴¹⁶ The draft *National Defence Space Policy* clearly reinforces Canada's commitment to non-weaponization. Unfortunately, that commitment means that many of Canada's most vital military space assets (including those that are either nationally owned or accessed) are vulnerable to both kinetic and non-kinetic attack. That vulnerability cannot be resolved by diplomacy and international agreements alone, as access to space extends well beyond national governmental space programs. In a trend expected to continue, more and more organizations and wealthy individuals are able to access space without

416. Specifically, the treaty outlaws the use of "nuclear weapons or other weapons of mass destruction." WMDs can pass through space en route to a target, as long as they do not become trapped in orbit.

the support of nation-states for financial backing and provision of Space Support infrastructure. Space Support technologies enabling space-lift and satellite operations are becoming increasingly pervasive and inexpensive. As Army reliance on space increases, so too does the number of players in space. Although space is by no means crowded, it is increasingly being populated with satellites of disparate origins and purposes. Space is therefore becoming more and more contested.

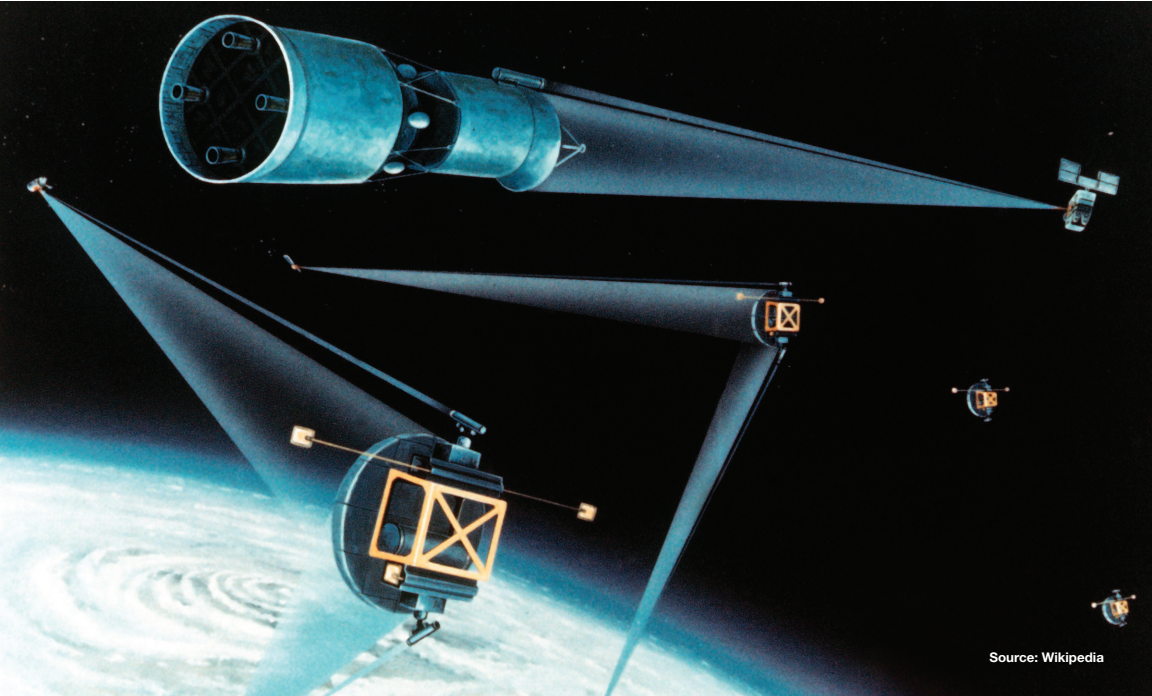
The draft *National Defence Space Policy* allows Canada to pursue protection measures for space assets. Accordingly, space assets may be engineered to optimize both detection and collision avoidance, while also being hardened against collisions and interference. The draft *National Defence Space Strategy* goes even farther, stating that measures for the purpose of self-defence, or to deny adversaries the ability to project space effects may be taken so long as they are temporary, reversible, and localized. Presumably the measures referred to are orbital manoeuvre techniques (such as co-orbital rendezvous) and the use of directed energy weapons (DEWs) and electronic attack (EA). These latter measures, however, may constitute weaponization of space—regardless of whether DEWs or EA originate in space or of the fact that they do not intend to physically destroy their targets. DEWs and EA are quite capable of transforming functioning satellites into space junk, and the probability that they will cause permanent damage to adversarial satellites is by no means remote.

War in space is improbable—it is too expensive and its consequences are likely to be in nobody’s best interest. Nation states and terrorist organizations alike heavily rely upon space-derived capabilities for command and control, ISR, and other force enhancements. The cyber route is likely the easiest way in; therefore, it is imperative that all cyber-electromagnetic gateways be heavily defended.

If space-based capabilities are truly essential to the conduct of operations, then a capability gap exists in our ability to protect and defend those assets. Should space-based assets be rendered inoperable, the Army would lose many of its Space Force Enhancement capabilities. That is an area of key concern in which a future multi-domain solution will be essential in closing the potential space gap.

PART FOUR – MULTI-DOMAIN CONCEPT

The first domain to consider in deriving a multi-domain solution is space itself. Redundancy in space may be developed by forging commercial and civil partnerships as well as technical and military partnerships with other nations. Any improvements to Space Force Enhancement functions by space

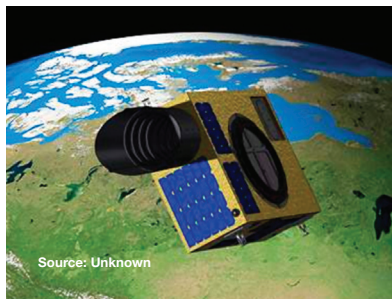


Source: Wikipedia

partners must be fully supported by the CA, so long as capability improvements match up well with actual requirements.⁴¹⁷ Although the development of a Space Control capability is not suited to Canada's Army, the CA must be a staunch supporter of Space Control measures that contribute to assured access of space-derived capabilities—without advocating space weaponization. Space Control techniques include cyber and EM shielding along with other Space, Link and Ground segment protection measures, as well as non-military solutions, such as prevention.

417. The CA requirement for each Space Force Enhancement function is not stated here if such a requirement has been stated elsewhere. For example, the Army C4ISR requirement is defined by the CAF ISR WG, led by Director General Integrated Force Development, and the Army C4ISR WG, led by the Director General Land Capability Development.

Technological development in the area of small satellites—especially those weighing less than 100 kilograms—holds a tremendous amount of promise for the Army.⁴¹⁸ Small satellites can be launched using highly mobile launch facilities. They may be used in support of particular theatres because they can be launched from any location. Small satellites would contain small quantities of onboard fuel so as to facilitate ease of launch and orbital emplacement, and would therefore be used for those missions where long endurance is not required. Despite their small size, they must be supported while on orbit; therefore, they must be placed in an orbital type best suited for satellite operations (e.g., GEO) or in an orbit where satellite lifetime can be minimized (e.g., LEO). Small satellites have great potential as a reliable means of communications relay (for computer networks or sensor nets) or persistent overhead ISR. Though they hold tremendous promise, there is much operational research and R&D left to do before such systems may be considered for use by the CAF.



A multi-domain solution that delivers what we presently term Space Force Enhancement capabilities must include more than just space-based systems. There may be innovative uses of air- and ground-based platforms or systems that contribute to a redundant solution, or there may be a requirement for novel materiel solutions. Multi-domain planning may be informed by the PACE (primary, alternate, contingency, emergency) technique. Although not a part of Canadian doctrine, PACE planning can be a useful construct for the Army.⁴¹⁹ For example, critical space-derived imagery from a particular satellite constellation must be backed up by similar capabilities on other constellations (whether national or foreign, military or commercial). Similar capabilities could also be present on air platforms, both manned and unmanned. Because unmanned platforms rely on SATCOM for command and control, they must be backed up as well. High-altitude, long-loiter platforms—including, for example, dirigibles and ground-controlled UAVs—are another domain capable of providing imagery of similar quality to

418. Small satellites include mini-, micro-, nano-, and pico-satellites. Mini-satellites have a mass between 100 and 500 kilograms, including fuel. Micro-satellites have a mass between 10 and 100 kilograms. The mass of nano-satellites is between 1 and 10 kilograms; that of pico-satellites is less than 1 kilogram.

419. PACE planning is an integral part of US doctrine. As standard operating procedure, units identify their critical systems, including weapons, communications, logistical, and medical. They then designate the alternate, contingency, and emergency backups in the event that the primary system becomes disabled.

contemporary space-derived products. Further analysis is needed to determine the right mix of ISR sensors, across multiple domains, which the Army will need in the future.



PNT is a space-derived capability that presents more of a PACE planning challenge than ISR, because the commercial and military R&D communities have not devoted as much time and effort to building redundancies into the PNT process as they have into the ISR process. Other sources of PNT information, such as LORAN, VOR, and NDB, have fallen out of favour since the USA turned off GPS selective availability in 2002.⁴²⁰ The shift toward full reliance on GPS has troubling military implications given how easily GPS

420. These particular electronic terrestrial navigation systems are not regarded as cost-effective. It makes little sense for governments to maintain multi-million-dollar terrestrial PNT systems when GPS broadcasts the same information, with a higher degree of accuracy and global coverage, free of charge.

signals can be jammed.⁴²¹ Positioning and navigation need not be the sole purview of the GPS system. There are other global navigation satellite system (GNSS) constellations such as GLONASS (Russia), Galileo (European Union), COMPASS Navigation System (China), and IRNSS (India) which Canada may be able to exploit in the future. Although space-derived PNT may be acquired by Canada through international agreements and partnerships—and free services—that does not ensure access.

Canada does not necessarily need assured access to space to meet its PNT requirement in the future. A system of air- and ground-based repeaters, using stellar measurements, caesium clock technology, inertial navigation software, and dead reckoning may be able to mitigate the loss of space-derived PNT in the future.⁴²² Such a system would ensure access for the Army to PNT data essential for command and control, computer network operations, decision making, situational awareness and understanding, friendly force tracking, navigation, and mapping. Of course, such a system would not have the advantage of coverage that GPS offers but could provide effective coverage across a limited area of interest. Because a PNT receiver needs to be within line of sight of at least four other PNT broadcast stations (in order to solve for the four unknowns in the PNT equations: latitude, longitude, altitude, and receiver clock bias) space offers the distinct advantage of the largest possible fields of view and minimum interference from obstacles. A combination of PNT broadcasts from high-altitude platforms (including UAVs, micro-satellites, or airships) coupled with dead reckoning, inertial navigation software, and ground-based broadcasters and repeaters may provide a solution.⁴²³

SATCOM involves the same PACE considerations as PNT does. Having the ability to communicate on multiple space-based systems is imperative and is a cornerstone of modern land operations. Building in redundancies by exploiting existing network infrastructure for rebroadcasting, repeating, retransmitting, and routing is one possible solution. The Enhanced Position Location Reporting System (EPLRS) radio offers this functionality today, acting as a repeater and an IP-based router for tactical communication networks. The HF pathway represents another possible backup for SATCOM,

421. GPS III, the latest update to the GPS constellation, includes several upgrades worthy of note here. They include improved PNT accuracy with more signals and more power (including spot beams that provide anti-jamming capability to military forces).

422. Such technologies are being developed for unmanned ground vehicles to compensate for their operations in GPS-denied environments like tunnels and urban structures.

423. Such a system should not be a stand-alone network, but should ride on existing infrastructure. For example, the SASNet, a sensor network currently undergoing research and development in DND, may provide the backbone required for such a ground-based broadcast system.

although the Army has divested itself of much of its HF capability. Line-of-sight communication systems, through combinations of ground-based and air-based nodes and platforms, may offer further redundancy. High-altitude UAVs and airships can also reduce the Army's dependency on SATCOM. For rear link communications, the ability to tie into a wired telecommunication system should not be ignored, though it necessitates robust communication security protocols along the entire signal pathway.



PART FIVE – NOVEL USES OF SPACE

5.1 IMPOSSIBLE APPLICATIONS

Before exploring some novel uses of space, it is worthwhile to mention some applications that cannot be conducted from space. (Note: Although many areas of Space Force Application are illegal under international law, they are still physically possible.) Some impossible applications include the following:

- **Full Motion Video (FMV).** Though FMV is possible from manned and unmanned aircraft operating in Earth's airspace, such video cannot be captured from the medium of space itself. Simply put, because satellites move so rapidly relative to the Earth, FMV would be necessarily short in duration and non-uniformly slanted (because of the camera angle in relation to the planet's surface). These problems could be overcome by using a camera in GEO orbit and taking video of the point directly below the satellite (i.e., the zenith). However, that would be an extremely limited application of space technology, unless military operations were being conducted directly on the equator and were unobscured by tropical rainforest.

- **Instantaneous Imagery.** Much the same way that FMV is constrained by the laws of orbital mechanics, so too is the ability to obtain instantaneous imagery. For imagery to be useful, it must be taken from overhead—or as close to overhead as possible—as to avoid obstacles in the line of sight and to minimize shadowing and skewed perspective caused by the slant factor. Imaging satellites may always be within line of sight, but they are not always directly above the target.

5.2 SPACE-BASED ROUTING⁴²⁴

Space-based routing may be thought of as “Internet everywhere.” The Army’s ability to conduct network operations—and therefore network-enabled adaptive dispersed operations—with space-based routers would greatly decrease the ground footprint of communications and information systems. With the communication hub in the sky, only a backup would be needed on the ground. The advent of mobile Internet has become commonplace through the proliferation of portable handheld devices like BlackBerry and iPhone/iPod. These technologies rely on a network of terrestrial-based wireless routers to obtain network access. For space-based routing to work, the same principles apply, but a couple of things need to happen before it will become viable:

- space routers need sufficient power (to overcome atmospheric absorption and terrestrial noise levels);
- mobile devices need sufficient gain (i.e., better gain increases an antenna’s ability to detect weaker signals).

5.3 DETECTING TERRESTRIAL BROADCAST

This may be thought of as “GPS in reverse.” GNSS technology works through the persistent space-based broadcast of signals that can be detected by Earth-based receivers. In reverse, the receiver would be located in space and the persistent signal would be located on the ground. Such technology is already in service for search and rescue operations. Applications here include friendly force tracking, adversarial force or target tracking (assuming the ability to tag the adversary or target in advance), and monitoring sensor feeds (creating a backup to terrestrial networks or delivering new sensor network capabilities).

424. These systems have already been designed and are currently undergoing testing. See, for example, <http://www.cisco.com/web/strategy/government/space-routing.html>.

PART SIX – CONCLUSION

The Canadian Armed Forces Integrated Capstone Concept document says that the “CF will need to expand its role in space to protect and exploit vital information and communication sources.” Space-derived capabilities greatly improve Army battlefield awareness, lethality, and survivability. They afford commanders the ability to virtually be everywhere on the battlefield at any given moment.

Much of the Army’s strategy and its future force employment concept is predicated on superior space capabilities. Reliance on space continues to increase even as space becomes a more contested environment. If the ability to conduct operations is contingent upon space dominance, then a multi-domain solution must exist in the event that space-derived capabilities are lost. The Army must therefore ensure that all of its essential space-derived capability can be acquired from other sources.

In summary:


- The Army cannot (and does not) support the conduct of Space Force Application functions that involve the weaponization of space.
- The Army should not involve itself in Space Support and Space Control functions unless the supporting technologies for these functions become significantly cheaper, more automated, and sufficiently mobile. It does, however, benefit from meaningful analysis of the SCOP.
- The Army will continue to rely upon Space Force Enhancement functions in the future, and therefore must continue to rely upon the CAF to leverage and develop partnerships (commercial, civil, and military; domestic and international) and assume risk.
- Risk can be mitigated by:
 - ▶ generating even more partnerships (bolstering redundancy);
 - ▶ investigating the possibility of inexpensive, automated, portable launch and control capabilities to support particular theatres;



Source: Combat Camera

- ▶ investing in multi-domain solutions where it makes sense to do so, including:
 - » high-altitude, long-loiter platforms;
 - » ground-based systems and platform technologies; and
 - » UAVs for surge capability; and
- ensuring that a measure of appropriate space expertise exists at the formation headquarters.

Space is expensive to exploit, yet is exceptionally difficult for an adversary to attack. The same principles that make it difficult to attack space-based assets make it difficult to defend them (with the added constraint of international law). Space is, however, the “highest of high ground,” offering persistence,



availability, and reliability advantages in enhancing functions such as ISR, communications, environmental monitoring, and PNT. In the future, space will offer capabilities such as space-based routing, friendly and adversarial force tracking, and remote sensor monitoring. All of these force enhancements make space an essential domain enabling the successful and decisive conduct of ADO.



CHAPTER 5

FUTURE ARMY CYBER CONCEPT



“... Nor is this new kind of war a game or a figment of our imaginations. Far from being an alternative to conventional war, cyber war may actually increase the likelihood of the more traditional combat with explosives, bullets, and missiles. If we could put this genie back in the bottle, we should, but we can’t. Therefore, we need to embark on a series of complex tasks: to understand what cyber war is, to learn how and why it works, to analyze its risks, to prepare for it, and to think about how to control it.”

—Richard Clarke, *Cyber War*

PART ONE – WHAT IS THE CYBER ENVIRONMENT?

At the strategic level of the Canadian Armed Forces (CAF), there has been much discussion recently of the nature of operating environments. In addition to the traditional land, air, and maritime environments, many strategists are proposing the introduction of new environments for consideration by military force developers.⁴²⁵ The CAF *Integrated Capstone Concept* (ICC) proposes three new environments (referred to as domains)—space, cyber, and human—while declaring that even more operating domains will emerge in the future. Specifically, nano and quantum are mentioned as possibilities.

The cyber environment, however, is nothing new. Rather, it is simply a unique manifestation of the electromagnetic (EM) operating environment—a familiar component of military operations with integral operating concepts and principles that lend themselves well to cyber.⁴²⁶

1.1 THE LAND, AIR, AND MARITIME ENVIRONMENTS

The traditional environments of land, air, and maritime are distinct and will continue to be distinct in the future. The division exists because different technologies—and therefore unique supporting equipment, skill sets, and training—are required to physically operate within these distinct environments.⁴²⁷ Sometimes the lines between operating environments can blur. The physical land environment, for example, may include water (swamps, streams, rivers, and landlocked bodies of water). Those features, however, differ significantly from blue water oceans. Blue water requires distinct technologies—both surface and subsurface—in which to operate. Land forces are ill suited to navigating maritime shipping lanes, and naval ships are similarly undesirable for swamp or riverine operations. Thus, land and maritime must still be treated as distinct physical operating environments.

Similarly, operations in the air environment require their own set of technologies. Dirigibles, fixed-wing aircraft and rotary-wing aircraft are all

425. The terms "environment," "domain," and "environmental domain" may be used differently or synonymously depending on the source. The lack of common language is often what stirs debate on such conceptual issues.

426. The term "domain" will be used to describe a sphere of influence. For example, the land domain may refer to those things which can be influenced by the land component commander. Domains are not necessarily restricted to influence by one person but may be influenced by any number of different things (hence forming an infinite set of domains). The cyber domain, for example, may consist of the physical space influenced by actions in cyberspace—anything from blogging to computer network operations.

427. This technology-based conceptual distinction between operating environments was drawn by Regan Reshke, Chief of Staff Land Strategy Science Advisor, during Land Concepts and Designs (DLCD) discussions concerning the nature of the human dimension in March 2010.

technologies required to operate in the air environment, yet they are completely unsuited to maritime or land operations (although they are essential to *support* both land and maritime operations). Army brigade groups or naval task groups may be structured to include helicopters in their respective orders of battle, but that is a characteristic of joint operations rather than an example of merging physical environments. The use of distinct technologies to delineate physical operating environments opens up other possibilities for environments beyond land, air, and maritime. As distinct physical components, only space and cyber need be added to round out an all-inclusive model of the physical plane.

1.2 WHY SPACE IS AND WHY HUMAN IS NOT⁴²⁸

Should space be considered as a separate environment from air, or is there just one aerospace environment? The answer essentially rests on one's definition of the term "operating environment." Although several definitions exist, each with its own nuances, an operating environment may simply be thought of as the milieu in which military activities are conducted.⁴²⁹ Operating environments may be distinguished from one another based on the technology used by military personnel to operate in them. Based on this definition, air and space are indeed separate (planes and satellites, for example, tend to work well in one of those two environments and not in the other).

Although space can be distinguished from the air environment (indeed, some argue that they are physically separated by the Carmen line itself), it becomes more difficult to conceptually differentiate cyber. Indeed, there exists a fair degree of misunderstanding about what is meant by cyber. Often it is confused with virtual reality or seen as something that exists on the information plane. The information plane, however, is not a physical environment; it is simply the link between activities that take place in the physical plane and effects that are achieved on the psychological, cognitive, and moral planes (which together may be referred to as the human dimension). Cyber is physical in that it manifests only through the actual manipulation of electrons and electromagnetic energy.

The Integrated Capstone Concept (ICC) fails to mention the electromagnetic (EM) spectrum in its treatment of operating environments. Indeed it fails to mention EM at all. It is understandable that the document included no

428. The discussion in this section is based on DLCD discussions concerning the nature of the human dimension in March 2010.

429. For example, the ICC describes an operating environment as "where elements of power and influence are exercised." It lists maritime, land, and air as some of the domains within this environment. This language is contrary to existing terminology of land, air, and maritime environments.

discussion of potential future environments such as nano and quantum, since we do not yet operate in such environments, at least not intentionally. Given that we have been exploiting the EM spectrum for military purposes for more than a century, it is surprising that the ICC gave it no consideration. It did, however, pay considerable attention to the human domain, an area outside the traditional breakdown of the physical plane.

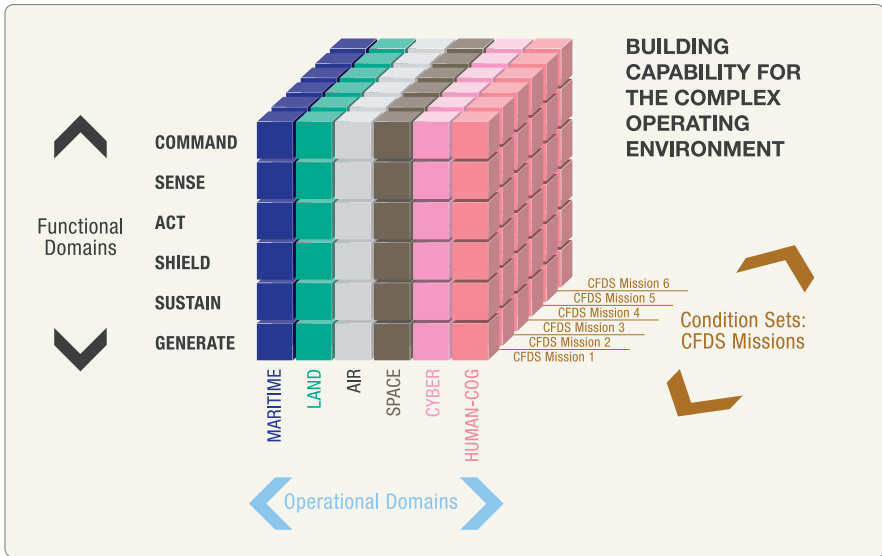


Figure 5.1.1: Emerging Environments

In the model proposed in the ICC at Figure 5.1.1, the human environment is represented in the same manner as land, maritime, air, space, and cyber. The model’s intent is to draw attention to the human dimension of military operations, but delineating the human as an operating environment actually undermines the overarching importance and omnipresence of the human, thus defeating its objective of elevating the human dimension above the physical operating environments. It can certainly be argued that the human mind is an operating environment on the cognitive, psychological, or moral plane (each of which are underpinned by physical processes within the human brain), but such an argument overlooks the actual intent underlying the need to distinguish between operating environments.

Figure 5.1.2 shows the traditional depiction of the effects-based approach (EBA) to planning and operations. The EBA model may provide a better framework for situating the human dimension within an operational context.

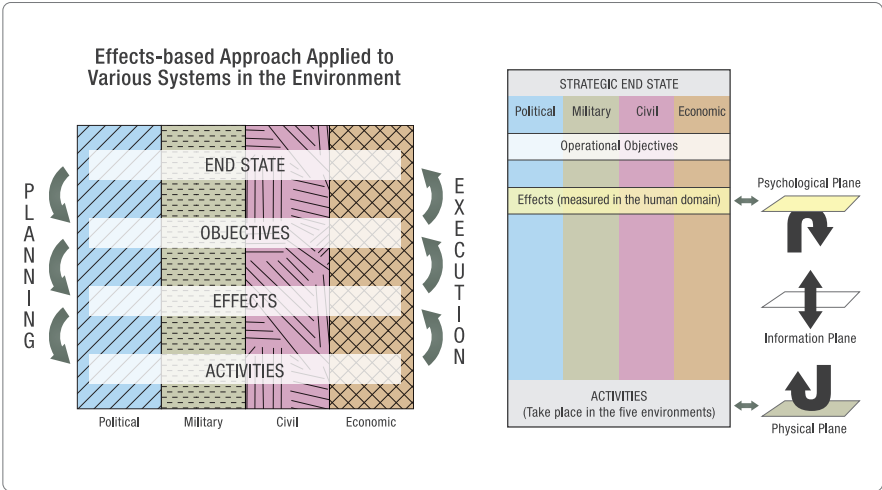


Figure 5.1.2: The Effects-Based Approach to Operations Model and the Human Dimension

Figure 5.1.2 and the follow-on notes attempt to explain this approach.

If “environment” is defined as the physical milieu within which activities are conducted, then a comprehensive list of environments need only include land, maritime, air, space, and EM. These five environments are valid in that they each require their own set of unique technological operating capabilities—again, that is why space must be considered as being separate from air. Activities conducted within these environments occur in the physical plane, and effects are generated across the physical, information, and psychological planes. However, when considering the EBA, the emphasis of effort is directed at analyzing effects on the psychological plane. It is on that plane that effects have the highest payoff, because it is there that the human dimension (formerly called “human domain”) dominates.

Activities may have first-order effects on the physical and information planes, but the milieu where effects matter most is on the psychological plane, for this is where adversaries’ understanding is shaped, their will undermined and their cohesion shattered; where domestic opinion and operational legitimacy lie; where trust within the comprehensive approach is built; and where so-called “hearts and minds” of local populations are influenced. Therefore, Figure 5.1.2 may serve as a more comprehensive framework in which to envision the all-important human dimension. In this model, all activities conducted within the five physical environments are prosecuted with a view to achieving desired effects in the human dimension, across all operational themes.

The human dimension is pervasive. The physical environments are merely the milieu within which activities are conducted to affect this human dimension.

1.3 THE ELECTROMAGNETIC OPERATING ENVIRONMENT: HOW CYBER FITS

Any given publication on the cyber domain will yield a unique definition of the term “cyber.” Within Canadian Armed Forces doctrine, there is no prescribed definition of “cyber,” at the time of writing. Therefore, it is worthwhile at this point to explore some of what the CAF has said about cyber to date.

The ICC describes the cyber environment (or cyberspace) as consisting of the Internet, telecommunication networks, computer systems, and software:

The cyberspace environmental domain will be a mechanism for integrating all of the environmental domains at the strategic level resulting in one common operational picture of the mission environment. This functionality will be complemented by the facility of the cyberspace environmental domain to merge the strategic functional domains, producing integrated effects. Cyberspace may also be where the medium and the message are virtually inseparable.⁴³⁰

Thus the ICC, while acknowledging that cyber rests on the physical plane, argues that it also encompasses the information plane. That statement confuses the purpose of the information plane and disregards the fact that all activities conducted in the physical plane are meant to generate information that will achieve an effect in the human dimension. Cyber is but one of several physical operating milieux exploited in the conduct of information operations; and the term “cyber” itself ignores other EM considerations.

The ICC hits upon a key point that unfortunately is not expanded upon: that the cyber environment encompasses telecommunication networks. As mentioned already, the ICC describes cyberspace as consisting of the Internet, telecommunication networks, computer systems, and software. Conceptually, software sits on computer systems which are connected via telecommunication networks creating a cyber world, as most readily exemplified by the Internet. Moving this idea forward, then, we need to think of what is physically going on within this conceptualization: the physical transmission of electromagnetic energy in order to physically manipulate electrons for the purposes of

430. Department of National Defence, A-FD-005-002/AF-001, *Integrated Capstone Concept* (Ottawa: DND Canada, 2010), 30.

conveying information. It is the interaction of energy and electrons that wholly describes this environment. As this is the same thing that occurs in the greater electromagnetic battlespace, we may regard cyber as simply a subset of an all-encompassing EM environment.

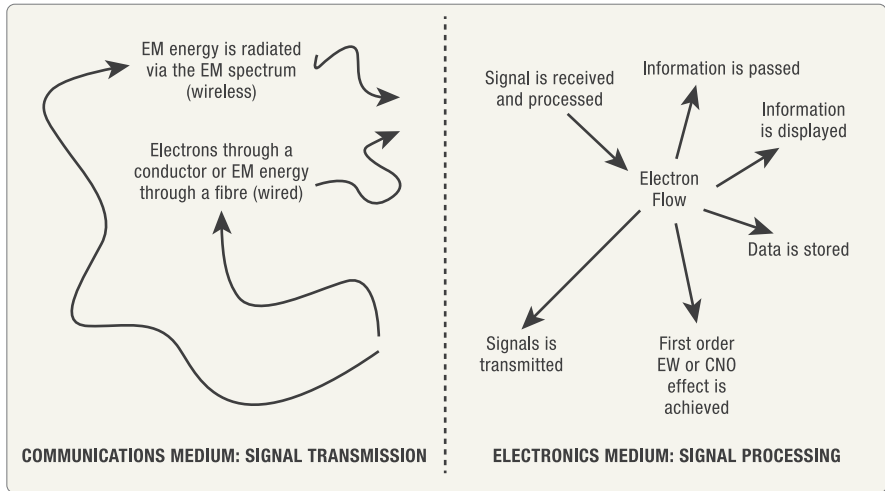


Figure 5.1.3: The Electromagnetic Environment

Therefore, there are precisely five environments: land, air, maritime, space, and EM. The technologies required to operate in each are distinct, and each environment requires its own unique supporting equipment, skill sets, and training.

1.4 COMPONENTS OF THE EM ENVIRONMENT

The Canadian Forces Communications and Electronics (C&E) Branch focuses on EM as its operating environment. With the advent of more and more advanced computer networks, the main effort of the C&E Branch has shifted away from radio and telephony toward intense focus on network operations that link together all so-called domains of the Branch.

As shown in Figure 5.1.4, the activities of the C&E Branch—collectively described as network operations—fit within the sphere of command and control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). The three domains of network operations include electronic warfare and signals intelligence (EW/SIGINT), communications and information systems (CIS), and computer network operations (CNO).

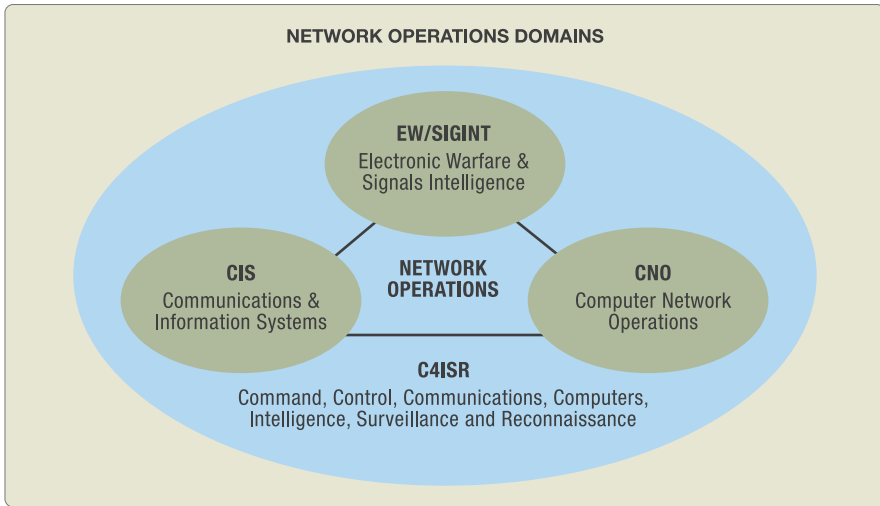


Figure 5.1.4: Network Operations Domains

Those three domains are linked by the physical EM environment, as depicted earlier in Figure 5.1.3. They are indeed inseparable, as a quick look at each of the domains will demonstrate.

EW is military action to exploit the EM spectrum. It encompasses the interception and identification of EM emissions; the employment of EM energy, including directed energy, to reduce or prevent hostile use of the EM spectrum; and actions to ensure its effective use by friendly forces.⁴³¹ The EW component is further divided into three sub-components: Electronic Attack (the employment of electromagnetic energy, including direct energy, to reduce or prevent hostile use of the electromagnetic spectrum and to ensure its effective use by friendly forces); Electronic Protection (action taken to ensure effective friendly use of the EM spectrum despite the adversary's use of EM energy); and Electronic Support (the search for, interception of, and identification of electromagnetic emissions in the EM battlespace). The products of electronic support include Electronic Intelligence and Communication Intelligence, referred to collectively as SIGINT.⁴³²

431. This paragraph is taken from *Electronic Warfare*.

432. Signals Intelligence (SIGINT) is the generic term used to describe COMINT and ELINT, either to represent fusion of the two types of intelligence or when there is no requirement to differentiate between the two. Electronic Intelligence (ELINT) refers to technical material and intelligence information derived from EM non-communications transmission (radar, navigational aids, jamming transmissions) by other than intended recipients. Communication Intelligence (COMINT) is technical material and intelligence information derived from EM communications and communication systems (morse, voice, facsimile) by other than intended recipients.

“CIS includes all the resources that bind all of the other components of the command and control system.”⁴³³ To be more precise, it is an assembly of equipment, methods, procedures, and, if necessary, personnel organized to accomplish specific information conveyance and processing functions. CIS encompasses both communications and computer-related resources including the associated low-level software applications. Communication Systems (CS) provide communication between users and includes transmission systems and switching systems in support of information transfer. An Information System (IS) is used by individuals to store, retrieve, process, and display information in support of job-related tasks. It includes software, applications, and processing devices such as computers, scanners, and printers; in other words, the Local Area Network (LAN) itself.

CNO comprises three components: attack, exploitation, and defence.”⁴³⁴ Computer Network Attack (CNA) includes the means to attack computer systems. Software and hardware vulnerabilities allow computers, storage devices, and networking equipment to be attacked through insertion of malicious codes, such as viruses, or through more subtle manipulation of data, all in order to affect the understanding, and ultimately undermine the actions, of the adversary. Computer Network Exploitation (CNE) supports Information Operations through the ability to obtain information about computers, computer networks, and the adversary by gaining access to hosted information and the ability to make use of the information and the computers and computer network. Finally, the purpose of Computer Network Defence (CND) is to protect against adversary CNA and CNE. CND is action taken to protect against disruption, denial, theft, degradation, or destruction of information resident in computers and computer networks, or of the computers and networks themselves.

Arguably, then, CNO could be a subset of CIS or even EW. However, it is important to describe CNO as its own domain within the EM environment, as that distinction allows us to define exactly what we mean by the term “cyber.” CNO consists of operations conducted within the cyber portion (or cyber domain) of the electromagnetic environment. Alternatively, the cyber domain ends where computer network operations are unable to achieve an EM effect. As communications and electronics technologies continue to merge, it is clear that the line separating CNO from CIS, and indeed the line between

433. This paragraph is taken from *Signals in Land Operations*.

434. This paragraph is taken from *Land Operations*.

CNO and EW/SIGINT, will cease to exist. In that sense, the EM operating environment will become wholly synonymous with the cyber environment.

The three network operations domains are exhaustive in that they include all military aspects associated with the manipulation of electrons and electromagnetic energy.

In summary, the EM environment includes electronic devices and their components (both hardware and software), the physical hardware connecting electronic devices, and the spectrum of electromagnetic energy itself (including all forms of radiation and EM particles—both elementary and atomic). Each specific domain within the overarching EM environment may include some or all of these components. For example, the cyber domain includes all communications and information exchange enabled by computer-based networks. In other words, cyber is the domain where computer network operations are conducted. That should not be confused with the term “cyberspace.”⁴³⁵ As CIS, EW/SIGINT, and CNO continue to merge, the cyber domain will expand to encompass all aspects of the EM environment. The process of expansion or envelopment, traditionally referred to as “convergence,” will eventually make the EM environment synonymous with the cyber environment.

1.5 THE CASE FOR NEW ENVIRONMENTS: QUANTUM

Given the definition of “environment,” is it reasonable to expect that new environments will emerge? The ICC mentions quantum and nano as potential candidates, while acknowledging that there may be other domains that we have not yet thought about.

“Quantum” refers to discrete packets of EM energy. Quantum theory is a different subset of physics than electromagnetic theory (though there is considerable overlap). However, that does not imply that a separate military physical environment is needed to describe activities and behaviour at the quantum level. It is the macro effect of quantum activities that is of interest on the physical plane. For example, futuristic quantum computing would be part of the cyber domain and hence the electromagnetic environment.

435. “Cyberspace” is a colloquialism used to refer to the virtual or online world created by the physical global cyber infrastructure. It is usually used synonymously with “Internet.” The cyber operating environment may include portions of cyberspace. For example, military operations may use cyberspace for intelligence activities, or they may simply exploit the physical public telecommunications infrastructure. It is worth noting, however, that the cyber operating environment is not the same as cyberspace.

The discovery of new spatial dimensions beyond the traditional three dimensions of the physical plane (up/down, left/right, and in/out) will fundamentally change our perception of physical space. In that respect, the word “quantum” is useful when referring to space beyond three-dimensional space or four-dimensional spacetime. When discrete packets of energy, called quanta, move from point A to point B, they do not move through physical space as we know it—rather, they follow all possible pathways from A to B (albeit some with greater probability than others). In simple terms, quanta seem to disappear at point A and reappear at point B without following a discernible physical pathway. Quantum tunnelling is a manifestation of this phenomenon. One might imagine a futuristic military application involving the conduct of operations within this quantum tunnel, i.e., in a higher-order dimension. However, no technological advance will allow us to pass formed structures through quantum tunnels (they are too big to fit!), which means that science-fiction applications akin to “Beam me up, Scotty” are extremely unlikely in the future. Quantum will therefore not emerge as a future operating environment.

1.6 A NANO ENVIRONMENT?

Another potential future operating environment put forward by the ICC is nano. Nano is a scaling factor that refers to a relative size rather than a place. Nano-science and nanotechnology therefore deal with behaviour and activities of physical entities at the nano scale (generally speaking, we may think of it as the molecular level). There are indeed unique technologies required to operate at the nano scale; therefore, at first glance, it appears to be a strong candidate for a future operating environment. However, it raises the question of whether or not the ability to conduct military activities in ever-shrinking milieux requires the emergence of new environments. For example, we currently have atomic warfare, yet it has not driven the requirement for the recognition of a separate atomic operating environment.

Nanotechnology best fits into the pre-existing operating environments in much the same way as described above for atomic weapons and quantum computers. Depending on the technological advance, nano devices (including their activities and behaviours) will simply fit into other domains. For example, nano weapons will affect operations in particular environments in much the same way as CBRN weapons do today. Therefore, they will simply be a component of the physical environment that they affect. In a similar vein, nano robots (or nanobots) will be part of the environment in which they work, be it land, maritime, air, space, or cyberspace.

Much as the maritime environment includes surface and sub-surface settings, the land environment logically expands to include the subterranean (as similar technologies and basing would be required in order to support both ground-surface and underground operations). The aerospace milieu is unique in that different supporting technologies are required for the conduct of military operations. Therefore, the physical setting above the Earth's surface is logically split into two separate and distinct operating environments. The electromagnetic nature of the physical world completes a holistic model of the physical plane of military operating environments. They constitute the sum of physical milieux where military activities can be conducted in order to convey information that will achieve effects in terms of shaping and influencing the human dimension—the ultimate objective of military operations at all levels. To be sure, technological developers need to continue to look at the physical world at scales much smaller than can be seen by the human eye, but such research into enhancing the human ability to operate in the five environments does not imply the emergence of new environments.

1.7 CONCLUSION

The discussion of operating environments must not be dismissed as merely theoretical. The purpose of clearly delineating the physical milieux of operations has a very useful application to the capability development process. Thinking merely in terms of how space and cyber support the land, air, or maritime environments creates the potential for vulnerabilities and lost opportunities. For example, if we think of cyber only as the glue that links Command with the other operational functions, we risk marginalizing the cyber component of the physical plane, turning it into a mere synonym for CIS—the so-called zeros and ones that only signallers should be concerned with. Thus we would miss the full range of force enhancement capabilities that cyber offers. When we examine the future security environment and consider the trend toward full convergence of cyber, EW/SIGINT and CIS, it becomes clear that an opportunity or vulnerability in one domain may be physically linked to exploits or threats in another. Therefore, a comprehensive understanding of what cyber is and how it fits into the traditional environments is essential.⁴³⁶

436. Author's note: Part I of Chapter 5 was originally published in the *Canadian Military Journal*, Volume 12, Number 3.

PART TWO – IS CYBER DETERRENCE POSSIBLE?

“If I’m not going to do anything other than improve my defences every time you attack me, it’s very difficult to come up with a deterrent strategy. We have to have a system that recognizes an attack, registers it and then allows us to react.”

—U.S. Marine Corps Gen. James Cartwright, Vice Chairman, Joint Chiefs of Staff⁴³⁷

The above quote from General Cartwright provides a logical place to start thinking about cyber deterrence and its relationship to offensive action. American military analyst Rebecca Grant recently stated that the United States must develop tough offensive cyber capabilities to use against its foes, arguing that “the best defence is a good offence.”⁴³⁸ American senior government officials have employed similar rhetoric.⁴³⁹ And they are by no means espousing an idea from the fringe. The idea persists that, in cyberspace, the best defence is a good offence. That idea just won’t go away—but it should. To be sure, offensive cyber operations offer some military utility, but such utility ought not to be confused with deterrence.

In the physical realm, offensive power often relates directly to deterrence. Deterrence involves manipulating an adversary’s behaviour by threatening them with harm, forcing them into a position where attacking is no longer an option worth pursuing. Traditional military deterrence concepts involve either (1) preventing an adversary from developing or obtaining a particular offensive capability or (2) possessing the capability to deliver such an overwhelmingly destructive blow that any potential adversary would refuse to engage in any sort of activity that might invite attack. The pre-emptive war in Iraq may arguably be a case of the former; the Cold War exemplifies the latter. The time has come for technologically dependent nations to examine how the concept of military deterrence works in the cyber environment.


2.1 OFFENSIVE CYBER CAPABILITY TO DETER CYBER WEAPONS DEVELOPMENT AND PROLIFERATION

The belief that a cyber offensive capability can be so robust that it can prevent potential adversaries from arming themselves with similar weaponry is false. For one thing, such weaponry is already ubiquitous. Other key factors

437. <http://defensetech.org/2011/07/18/dod-cyber-strategy-released/>.

438. <http://www.defensenews.com/story.php?i=3469918&c=AME&s=TOP>.

439. <http://www.washingtontimes.com/news/2008/sep/29/us-urged-to-go-on-offense-in-cyberwar/>.



contrary to this belief include the vastness of the Internet, the anonymity associated with the cyber environment, and the relative ease with which new cyber weaponry can be produced, reproduced, and disseminated. If you don't know who's building the weapons, where they are being built, or even what the weapons look like, no offensive arsenal of your own can achieve deterrence against weapons production and proliferation. Cyber weaponry can be detected only after it has been released, and by that time it becomes even more difficult to link it with the person or organization that actually released it. What would the Cold War have looked like if nations were incapable of knowing who had launched the missile and where it was actually launched from? There probably would have been a lot more missile attacks.

In order for an offensive capability to deter adversarial weapons development and proliferation, a surveillance and reconnaissance system is needed to locate production sites. Perhaps automated cyber tools could be developed that could search the Internet for potentially malicious code and then automatically neutralize it, but that concept is problematic for a number of reasons. Firstly, it would be impossible for an artificial intelligence (AI) to recognize a cyber threat unequivocally without having generated the code itself. Consider, for example, legitimate software programs that could also be used nefariously—such as another nation's cyber defences. The chances of friendly fire are high. Secondly, even if you did know precisely what your target looked like, the Internet is too big to perform persistent instantaneous searching across its entirety. Lastly, even if you could instantaneously search the Internet and accurately identify and defeat malicious code (through network isolation, quarantine of code, or some instantaneous Internet patching process), the overall affect on the Internet and its dependent systems would be unpredictable. In other words, the unintended effects could be disastrous for systems that you do not wish to disconnect or otherwise harm.

It must be assumed that nefarious individuals and organizations have the ability to arm themselves with cyber attack tools no matter how much offensive capability we develop ourselves. That raises the question of whether adversaries can be stopped from actually employing their capabilities once they are sufficiently armed.

2.2 FIGHTING FIRE WITH FIRE: OFFENSIVE CYBER CAPABILITY TO DETER HOSTILE CYBER ATTACK

Nor will conducting pre-emptive cyber attacks against a potential cyber adversary achieve deterrence. Assuming that an individual or an organization has been identified as a hostile cyber entity, it could be possible to disable the entity's network, corrupt its source code, or otherwise neutralize its offensive capability through a cyber first strike. There are several drawbacks to this type of approach.

Firstly, the problems of positive target identification and unwanted downstream effects still exist. Secondly, there is no guarantee that such an action would be effective, and there are no monitoring tools to conduct the cyber equivalent of a battle-damage assessment. In any event, restoring capability would not take long: copying an executable software program is much quicker than rebuilding a missile silo. Thirdly, revealing your attack capability by striking first makes it possible for the enemy to identify both their vulnerabilities and your techniques and procedures, thereby making it unlikely that any follow-on offensive action would be successful. Lastly, the inability to publicize offensive cyber operations cripples any ability to achieve deterrence. A victim needs to know who carried out the attack (or who holds the potential to do so) if the attacker is to be deterred in the future. Consider the words of British Armed Forces Minister Nick Harvey, outlining his cyber action plan: "In every other domain [of warfare] you have the concept of deterrence and ... in the fullness of time we would expect to get into a position where people understood our capabilities."⁴⁴⁰ A public declaratory policy, however, is unlikely because of the secrecy traditionally associated with cyber operations.

2.3 MUTUALLY ASSURED CYBER DESTRUCTION: A LOSING STRATEGY

A policy of public declaration existed during the Cold War: the United States and the Soviet Union made it clear that they each possessed a sufficient quantity of nuclear weapons to physically destroy each other and that they were willing to use them if the other side did so first. Therefore, a state of mutually assured destruction existed. The same situation cannot exist with cyber weaponry because the object of the threat is different. In nuclear war, the lives of the civilian population were at risk on both sides, and physical destruction for one meant the same for the other. This made attacking a losing

440. <http://www.canada.com/topics/technology/news/gizmos/story.html?id=561b3ebf-55ab-4348-9027-0d95762eb7aa>.

strategy, and consequently the nuclear arms race was validated as the best deterrence strategy.

Cyber weapons hold adversarial networks at risk. Publicly declaring that you hold cyber weaponry and are willing to use it against anyone who conducts, or shows intent to conduct, cyber attacks assumes that the adversary has as much to lose on their networks as you do on yours. In the nuclear situation, that is always the case. In the cyber environment, it is rarely the case.

The central tenet that kept the Cold War from turning hot—involving superpowers pitted directly against one another in armed conflict—was the idea of shared vulnerability and shared risk. In other words, nuclear weapons could not be deployed by one side in a timely or comprehensive enough manner to prevent the possibility of the other side launching its own nuclear arsenal. The use of nuclear weapons would therefore ensure that nuclear weapons would be used against you, thereby achieving a condition of deterrence. That is not the case in the cyber environment, where vulnerability is not shared equally.

Technologically developed nations are heavily reliant on the Internet for almost all societal functions. Their economies and financial systems rely on it, as do business and industry. Critical infrastructures, including power, transportation and telecommunication grids, depend on it in order to function successfully. Even military forces, in pursuit of net-centric warfare and information dominance, have become wholly reliant on computer networks that use Internet protocol and therefore connect to the Internet one way or another. The Internet consequently represents a tremendous vulnerability. By contrast, the technologically developing world does not depend on the Internet for its standard of living, though many such nations do enjoy a high degree of Internet accessibility. Interestingly, this technological divide is a consequence of economic disparity which is itself a root cause of conflict.

Many threat actors are not necessarily vulnerable to the effects of cyber aggression. For example, an underdeveloped nation state could have the means to attack a developed nation, but would be immune to retaliation in the cyber environment because its national and military infrastructure does not depend on it. Traditional military deterrence concepts therefore cannot apply. It does not make much sense to use an offensive capability that will have little or no effect on an adversary. A cyber weapons capability only holds cyber-dependent nations and their militaries at risk. Therefore, an

offensive capability is likely best employed in conflicts between technologically advanced nations.

2.4 DETERRENCE THROUGH REDUCING CYBER DEPENDENCE

Another way for technologically advanced nations to deter attacks is to reduce their reliance on cyber infrastructure. This would have the obvious effect of making such nations much less vulnerable to potential attackers. However, the risk that would be mitigated by such a strategy would be greatly eclipsed by potential losses in capability and productivity that cyber infrastructure provides in the first place. It is therefore, with good reason, unlikely that such a regressive idea would ever be palatable or desirable. That said, it is worth noting that an adversary cannot attack you if you do not present them with a target.

It is important to note here that many governments are taking steps to reduce the size of the target they present. By consolidating cyber infrastructure, the task of monitoring cyber defences becomes much easier. The consolidation of infrastructure, however, does nothing to reduce societal or organizational cyber dependence. Therefore, a reduced network footprint still constitutes a very lucrative target. Indeed, a successful attack would have the potential to inflict more harm against consolidated infrastructure due to lack of redundancy and network heterogeneity.

Given that technologically advanced nations will never reduce their cyber dependency, only a couple of deterrence concepts remain. Would-be cyber aggressors must be deterred by the fact that either (1) the cyber defence system is so good that any attempt at aggression would always be unsuccessful and therefore not worth the effort; or (2) acts of cyber aggression would bring physical military retaliation.

2.5 FORGET CLAUSEWITZ: DEFENCE AS DETERRENT

Building a cyber fortress is often touted as a viable deterrence possibility. The idea is that a nation can put together an impenetrable barrier which would repel all would-be attackers. Such a barrier would be based on infrastructure that focuses on security, rather than connectivity and interoperability, as the essential design principle. It would need new organizational structures and technologies for continuous monitoring and surveillance, defeating threats and exploits, and making iterative defensive improvements (e.g., patching

known vulnerabilities). However, even if such a fortress could be built, a good defence alone could not be a good deterrent because a good defence fails to put an adversary at risk. A cyber fortress mentality would only provide an incentive to attackers to be the first to knock the fortress down. All the attacker would risk would be time, patience, and money. The whole concept of “defence as deterrent” could be easily considered a wicked problem because a strategy designed to deter attack could conceivably achieve the opposite result.

In *On War*, Clausewitz said that it would be absurd to participate in “a war in which victories are merely used to ward off blows, and where there is no attempt to return the blow.” He cited many cases of nations that have lost wars because they engaged exclusively in defensive operations, though he did qualify his examples by noting that it would be wrong to say that the offence was never contemplated, it was just that the opportunity to conduct it did not present itself. Clausewitz might consider the cyber fortress a useful concept, as long as there were a set of conditions that under which offensive operations against the adversary could be conducted at some point in the future. In other words, if there is no retaliation, then there can be no incentive for the attacker to stop attacking.

As a final consideration for this sort of deterrence strategy, building a fortress implies making it very difficult for entities on the inside to connect with those on the outside. This, of course, undermines the purpose of being connected to cyber infrastructure in the first place. Certainly closed networks that do not connect to the Internet represent the hardest of cyber targets for attackers. But such networks are by no means impenetrable: they are vulnerable at every point where they take in information from external data sources. That includes physical hardware and software interfaces, electronic links, and human operators. The fortress alone cannot be a deterrent, but it can make for a terrific cyber defence. The best defence is good defence, not good offence. But defence alone cannot achieve deterrence.

2.6 CYBER DETERRENCE TODAY: A PIPE DREAM

Is deterrence hopeless? Without the ability to positively identify cyber adversaries and their weaponry (the problem of attribution), the answer, unfortunately, is yes. If we want deterrence, we must either find a technical solution to overcoming Internet anonymity or disconnect from the Internet altogether. As long as we continue to struggle with how to best solve the problem of attribution and retain our reliance on cyber infrastructure, we

must accept adversarial aggression in the cyber environment as a characteristic of the cyber environment itself.

2.7 AN INTERIM SOLUTION: WELCOMING ATTACK!

With no hope of deterrence (barring revolutionary technological advance or the implementation of new Internet protocols) the only option is to accept attack. In the interim, then, we must stop thinking about how to deter attacks and start thinking about how to defend against their inevitable occurrence and—knowing that we cannot stop them all—how to ultimately recover from successful ones.

Cyber defence consists of actions taken by military forces to protect against disruption, denial, theft, degradation, or destruction of information resident in computers and computer networks, or of the computers and networks themselves. This may be simplified by thinking of two guiding principles: reducing vulnerabilities and blocking known exploits.

Vulnerability may be reduced through the adoption of and adherence to modernized information system security practices. These include the traditional areas of physical security, communications security, IT security, emissions security, procedural security, transmission security, and personnel security, each with new associated activities that better address the growing vulnerability of the cyber environment to hostile actors. For example, personnel security measures have in the past largely been associated with military or departmental personnel and contractors only. It will become increasingly important in the future to look further back in the supply chain to assess the reliability of persons responsible for developing and delivering our hardware and software. Such potential vulnerabilities can also be addressed with technical and procedural checks on important cyber components prior to their use by military forces. Some nations are now making the move toward increasing domestic manufacturing capacity for certain pieces of hardware and software.

Context is important when considering the overwhelming challenge in the realm of cyber security. If you understand your vulnerabilities, you can reduce them. If you have information on a known exploit, you can block it. It follows, then, that you cannot defend against an unknown threat. Sometimes, even when you know about an exploit, it doesn't make sense to do anything about it. For example, the world's leading antivirus companies have the greatest

capacity for identifying malware. However, once malware is identified, there is a cost associated with neutralizing its effectiveness. A piece of malware may have ten lines of code. It may take a year before it is identified by a malware surveillance system, and then it may take thousands of lines of code to neutralize it. Then a malware writer can simply tweak a single line of code in the malware and continue to operate under the radar, wreaking havoc on computer networks for another year. That's a big investment into something that can be thwarted with such relative ease. For that reason, not all vulnerabilities are patched, even against known exploits. It simply is not practical to do so.

The US military is thinking about a different approach to defence. The Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) program currently being run by DARPA seeks to build computer systems modelled on the human immune system's ability to track down invaders, fight them off, and repair itself. As DARPA points out, even the most advanced computers are incapable of recovering on their own from attacks, either by finding new ways to complete their tasks or by repairing themselves. The human immune system, on the other hand, does that all the time.⁴⁴¹ A fully functioning CRASH network could welcome attack without any adverse effect on operations.

That would never preclude the continuous searching for potential vulnerabilities in the networks. So-called Red Teams do this now in organizations that place a high premium on security. Red Teams actively search for vulnerabilities and may even be employed to develop ways to exploit such vulnerabilities, all with a view to patching a defensive weak point before an adversary can find it. There is universal uncertainty about just how much damage exploiters can actually inflict once a network is permeated. Which information can they steal, modify, or delete? Which systems can they control? Which data streams can they redirect? The answers to those questions can only be found through the use of Computer Red Teaming, or with the help of well-intentioned white-hat hackers.⁴⁴²

Lastly, several attempts at formulating a computer network defence (CND) model in the force development community have borrowed from operational language. There has been debate over how one conducts a covering force

441. <http://www.popsci.com/science/article/2010-06/darpa-wants-secure-networks-inspired-human-biology>.
442. White-hat hackers probe systems for vulnerabilities and then inform network administrators of the problem. This is unlike black-hat hacking, in which vulnerabilities are exploited or passed along to other nefarious individuals or groups.

battle, a main defensive battle, or countermoves in the cyber environment. Borrowing from existing operational terminology and language is problematic because the cyber environment, although physical, is distinct. Defence in cyber is performed in a technical sense and does not hold opposing military forces at risk through violent offensive action.

2.8 DESTROY ANONYMITY: WELCOME DETERRENCE!

Clearly, then, the best defence is not a good offence. For now, the best defence is a good defence. Unfortunately, a good defence without the ability to hold the adversary at risk cannot be a deterrent. Only offensive capability can deter, but that is not possible if the adversary cannot be identified. When technology allows us to identify the adversary, offensive capability will work as a deterrent only if the adversary happens to be as dependent (or more) on their cyber infrastructure for operational success as we are on ours. If they are not, then the only military strategy that will deter them is the use—or the threat of—physical violence. Deterrence can only be achieved when anonymity is not possible. Once the anonymity problem is solved, a broad range of deterrents exist that must extend beyond the cyber environment.

PART THREE – OFFENSIVE CYBER OPERATIONS

The purpose of offensive operations is to defeat the adversary through the use of violence. Offensive action, on both the psychological and physical planes, through a combination of physical and intellectual activities, is the decisive operation of war, and through it ultimate success is achieved.⁴⁴³

Offensive operations may be conducted in any of the five physical environments: land, air, maritime, space, and cyber. Although the purpose and principles of offensive operations are captured well in existing land, air, and naval doctrine, there is no similar doctrine for the other environments. That is not surprising, given legal constraints and the lack of policy guidance for space and cyber. Canadian Armed Forces (CAF) capability developers are, however, highly engaged in exploring the way ahead with respect to cyber. While it is crucial that our cyber defence and intelligence capabilities continue to grow and evolve, there may not be a need to rush to enter into offensive cyber operations just yet.

443. The principles, characteristics, and purposes of offensive operations described here have been taken directly from B-GL-300-001/FP-001, *Land Operations*, Chapter 7, Section 5 – Offensive Operations.

3.1 OFFENSIVE OPERATIONS DOCTRINE

Offensive operations defeat the adversary by breaking their cohesion and destroying their will to resist. This can be achieved through the physical destruction of the adversary's forces, through synchronized disruption of their operations on the physical and psychological planes, or through a balance of both. Offensive information operations (IOs)—a subset of offensive operations—are conducted to physically destroy, attrite, disrupt, or deny the adversary the use of the electromagnetic spectrum and its supporting infrastructure. Offensive IOs include offensive cyber operations which contribute to the defeat of opposing forces by rendering them unable to accurately perceive situations, make decisions, or direct actions in a timely fashion.

The broader military community does not yet possess a good understanding of the options available to it for exploiting its adversaries through the use of offensive cyber action, largely because of security caveats and the difficulty of grasping exactly what is technologically possible when it comes to cyber weaponry. The latter can be partly righted by establishing and maintaining dialogue with trusted partners and by supporting our own research and development community. More importantly, however, the CAF needs to think about *why* an offensive cyber capability might be worthy of pursuit. In other words, once we know what we can do (technologically), we need to ask ourselves if it is worth doing (operationally) before any capability is actually developed.

3.2 POTENTIAL TARGETS FOR CYBER WEAPONS

Conceptually, in developing a rationale for employing cyber weaponry, we must first determine the type of military target that could be susceptible to cyber attack. Typical military targets include conventional and non-conventional forces as well as civilian populations and infrastructure. Once we understand which target sets we can actually affect, we must then determine the likelihood of actually attacking such targets. If the types of targets that we can significantly affect are likely to be the types of targets we expect to encounter in future operations, then investment in offensive cyber capability is warranted. If not, the CAF should assign low priority to capability development activity related to offensive cyber weaponry.

For an offensive cyber attack to be worth the effort, it must be capable of delivering a significant blow to an adversary's network. Therefore, the primary

consideration when developing a network attack capability is the degree to which potential adversaries are reliant on cyber capabilities. If the enemy does not depend on their network to fight, then attacking it will likely yield very limited payoff for the CAF. If the enemy uses a net-centric approach to operations, cyber attack could be the most effective way to defeat their combat power. (Incidentally, that ought to set off alarm bells about the absolute requirement for the CAF to have a robust network defence capability.)

Non-conventional adversaries do not adopt a net-centric approach to operations. They use the Internet for spreading propaganda, for recruiting, for training, and possibly for launching cyber attacks against us. It is fair to say that they do not rely on information systems to anywhere near the same degree that we do for operational C2, tactical situational awareness, battle management, and passage of information. For the most part, they tend to use other electronic devices to execute command and control. Attacking Internet infrastructure that hosts non-conventional adversaries is therefore not a winning strategy. A cyber attack is unlikely to limit adversaries' C2 to any significant degree and would most likely just push them to another corner of the Internet. Although they expose themselves to the possibility of exploitation by operating on the Internet (via network intelligence activities and, arguably, through deception), non-conventional adversaries do not present a clear target for offensive operations in the cyber environment.

The easiest target for offensive cyber weaponry may be critical civilian infrastructure. The degree to which such infrastructure is vulnerable to network-based attack is directly proportional to its dependence on Internet connectivity. Put simply, if critical infrastructure is connected using Internet protocol (IP), it may be attacked via the Internet, albeit with varying degrees of difficulty. Rather than dropping a bomb on a power plant, for example, a cyber attack could be used to disrupt the plant's IP-based supervisory control and data acquisition systems, thereby crippling power production and minimizing overall physical destruction. Indeed, much of the literature on cyber warfare is heavily focused on such scenarios, where the threats posed to domestic critical infrastructure by malicious individuals and organizations are translated into possible options for military operations. The use of cyber weapons to target critical civilian infrastructure would have to be considered in the same manner as any other physical weapon system, with a mechanism that ensures that only legitimate military targets are attacked and that every effort has been made to minimize collateral damage. With all that said, however, the use of cyber attack against another nation's critical infrastructure,

though possibly allowing for military advantage, will likely invite retaliatory action against one's own nation and is therefore probably not worth pursuing.

Conventional threats in the form of regular militaries present a much more likely candidate for attack via offensive cyber operations. Conventional militaries are the most likely to exploit network capabilities in everything from logistical support and force projection activities down to tactical-level command and control and information exchange. This makes such an adversary a lucrative target, as even a relatively basic cyber attack could achieve operational success by generating effects across the physical and moral planes.

As mentioned, from a capability development perspective, it makes sense to invest only where the highest payoffs are likely. Therefore, we must understand the type of adversary that we are most likely to fight in the future before committing to CAF investment in offensive cyber capability. According to the future security environment (FSE) document released by the Chief of Force Development back in 2009, confrontation with non-conventional non-state actors will be the most likely form of conflict in the near future. Cyber attack may therefore have little payoff in any offensive CAF operation conducted against such adversaries. The FSE document also suggests that operations will most likely take place in failed and failing states, locales likely unsuitable for any sort of IP-based attack on critical infrastructure. However, the FSE document rightly asserts that conflict with conventional armies remains a possibility, and therefore the CAF must have the right mix of offensive capabilities to deal with that type of threat as well. It is there that cyber weapons can potentially deliver a high payoff.

In a 2007 airstrike against a suspected Syrian nuclear facility, it was widely reported in various open sources that the Israeli military had allegedly used a cyber weapon to successfully suppress Syrian air defence systems. Cyber attack allowed the military to achieve surprise and effectively avoid the political consequences that would have come with collateral damage from the physical bombing of air defence installations. Suppression of enemy air defence is one example of an offensive activity that can be conducted in the cyber environment against a conventional force. The potential to shut down everything from the enemy's C2 systems to their actual weapon systems is already largely possible today. As technology advances and nations become even more connected, the possible targets for cyber attack will increase in lockstep.

If conventional military forces of nation states were the threat most likely to be encountered in the future by the CAF, then significant investment in cyber attack capability would be wise. However, that it is not.

3.3 CYBER INTELLIGENCE

Some security analysts have justified the development of offensive cyber capability as a necessary counter to the threat of hostile cyber attack. However, that idea, known as the deterrence model, only confirms the requirement for strong network defence. Just as it is not necessary to use chemical attack against an adversary that employs offensive chemical warfare against us, it is not necessary to fight a cyber-attacking adversary with a cyber attack of our own. The CAF, however, does need a chemical defence capability. Similarly, because everyone connects to the Internet, the CAF requires a robust, resilient cyber defensive capability throughout its force. Moreover, such capability can be markedly improved by a robust cyber intelligence capability.

Growing interconnectedness and network reliance on the part of most nation states and non-state actors alike should compel the CAF to make a significant investment in its network defence capabilities, for any adversary is likely to attack or exploit it in the cyber environment. Similarly, investment in network intelligence and exploitation capabilities can offer considerable payoff across the continuum of operations and against all manner of adversarial actors.⁴⁴⁴ There is a great deal of uncertainty, however, when it comes to the development of an offensive cyber capability. Such development would not come cheap. It would require significant investment in an area of warfighting expertise that is unlikely to be used much, which implies that investing in this particular area carries a significant risk. It would likely be more advantageous to put valuable CAF resources to better use elsewhere. Such a risk is not present in cyber defence and intelligence capabilities, where investment makes a great deal of sense.

Luckily for the CAF, investment in one capability may represent an opportunity for rapid development of another. Specifically, fostering an intelligence capability could lay the groundwork for building an offensive capability should circumstances warrant it.

444. Much like the employment of an offensive capability, the use of any sort of exploitation technique must be in accordance with relevant policy and legal constraints.

The conduct of intelligence gathering has been a feature of the cyber environment since the environment's inception. Like any other electronic communications and information medium, the cyber environment has been and will continue to be an active area of operations for intelligence collection. Put simply, electronic environments allow for the passage of information that is highly vulnerable to interception. Because the information pipeline represents a physical connection with a military force, it can also represent an attack vector. The electronic environment must be defended accordingly, in order to protect both information and the force itself.

The cyber environment makes intelligence gathering a lot easier than traditional methods permit. Techniques of such cyber espionage include the laying of electronic trapdoors which establish an entry point into intelligence-rich computer networks. It is not a huge technological leap to exploit a trap door for the purposes of offensive cyber operations. Rather than a simple portal that allows probing, snooping, spying, and copying, the trapdoor could be used as a foothold into an enemy network for the conduct of offensive cyber activities: deleting or altering information, spoofing or disrupting operations, and even destroying infrastructure.

3.4 CONCLUSION

A force that is trained to conduct cyber intelligence gathering may be easily re-rolled into an offensive entity should circumstances warrant such a transformation. Although it probably makes operational sense for the CAF to have some offensive cyber capability, it must necessarily be centralized and narrow in both size and scope given the limited resources available to the CAF and the actual nature of the threat. Should the threat picture change, investments already made in network defence and intelligence capabilities would position the CAF well to have the resiliency it needs to adopt an offensive cyber posture. For now, the emphasis must absolutely be on cyber defence.

PART FOUR – ARMY CYBER CONCEPT

Traditionally, telecommunications users needed a hard-wired copper connection to connect their device to the telecom infrastructure. Satellite technology allowed an expansion of edge devices and supporting infrastructure. This has evolved even further to include mobile cellular devices which connect to the telecom infrastructure via radio waves and cell tower networks. The Internet, brought to homes and businesses via those same telecom connections, is now

accessed routinely from mobile edge devices. Beyond smart phones, there are assisted-GPS tracking devices, 3G security cameras, urban traffic control systems, supervisory control and data acquisition sensors, home control and automation systems, and even vehicles which connect to computer networks through wired and/or wireless telecom connections. The ease of access to cyber infrastructure means that, like most technology, it can be easily exploited for either productive or destructive purposes. While there are ever-expanding opportunities for information sharing and the productive use of smart computing, the threat to such cyber architectures continues to grow apace.

“Cyber” is a new term in the defence lexicon. But regardless of how it is defined, cyber itself is nothing new. As one manifestation of the broader electromagnetic environment, the cyber domain may be largely regarded as the milieu where computer network operations are conducted. As more and more computing devices become embedded in the physical environment around us, the cyber domain will continue to expand.

The convergence of information networks and wireless technologies introduces considerable vulnerability to the Army network environment (ANE). This convergence has exposed several gaps in the Army’s ability to both protect its own information systems and exploit those of the adversary. Traditional CNO and EW activities cannot close those gaps on their own.

4.1 CNO AND EW: NO LONGER DISTINCT

Computer network operations must be integrated with communications and information systems, electronic warfare, and signals intelligence into one coherent cyber operations domain in order to exploit technological convergence and existing synergies between these different mission sets.

The targets of CNO and EW are rapidly converging into one target set. Computer network operations (CNO) is that domain of military activity which comprises, among other things, exploitation of and attacks on adversarial computers and computer networks. Electronic warfare (EW), on the other hand, largely involves the manipulation of adversarial electromagnetic energy through signal intercept, analysis, exploitation, spoofing, jamming, and so forth. It is clear that influencing an adversarial wireless information network involves more than the application of either CNO or EW doctrine: it requires both. It therefore makes sense to merge these military activities into one coherent domain of cyber operations.

The converse is also true: Army TacC2IS and Army TacComms have merged into one system of systems. Thus, a vulnerability in the one may present an exploit in the other. The Army network environment must be defended accordingly. As mentioned in the first chapter, cyber has now encompassed most of the EM environment and soon will envelop it to such an extent that the terms “EM environment” and “cyber environment” will become synonymous.

**4.2 CYBER OPERATIONS = COMPUTER NETWORK OPERATIONS
+ ELECTRONIC WARFARE**

Consider various computer network configurations for battle command systems or military information networks in general (enemy or friendly, each containing combinations of COTS, MOTS, and GOTS hardware and software):

- **Cyber-Fortress:** a closed internal network in a static headquarters using only wired connections.
- **Cyber-Dispersion:** The fortress model is extended through secure wireless technology to soldiers on the battlefield.
- **Cyber-Parasite:** The network (or parts thereof) relies on the commercial telecom backbone for connectivity.
- **Cyber-Enclave:** The network connects to the Internet, may contain some sort of firewall and security infrastructure, and may contain both wired and wireless components.

For obvious reasons, the cyber-enclave is an easy target of both EW and CNO techniques. The cyber-parasite is a potential target of CNO techniques, as its traffic rides a commercial backbone. If that backbone includes any sort of wireless link, it could also be potentially targeted by EW. The dispersion network could also potentially be exploited by EW and CNO techniques.

Only the cyber-fortress cannot be penetrated using traditional EW techniques. There are, of course, several CNO techniques which could be used to penetrate this network (think Stuxnet). Though the fortress is safe from electronic support techniques (unless wireless hardware could be installed on the network through actual physical access), it is still vulnerable to EA. So, although a distributed denial of service (DDoS) attack might not be possible,

an EMP attack could prevent network components from communicating with one another.

Cyber operations consider all possible vulnerabilities—friendly and adversarial—and use techniques from all military domains to protect and defend, to support and exploit, and to attack. For example, consider an enemy emitter that is networked to a GPS device. EW assets may be tasked to direction-find (DF) the emitter by searching the EM spectrum for the radio waves it broadcasts and then geo-locating the origin of the wave. A CNO capability, on the other hand, enables DF by using cyber techniques to “ask the emitter where it is.” Both courses of action represent viable and complementary ways of sensing an adversary’s presence and intent. Breaking down stovepipes, a cyber operation might include ES finding, CNE fixing, and EA or CNA striking.

4.3 THE CONTEXT OF CONVERGENCE: C4ISR AND THREAT

The Army is heavily reliant upon computer and electronic communications networks both for the command and control (C2) of deployed forces and for intelligence, surveillance, and reconnaissance (ISR) activities which provide operational information to a highly dynamic and decentralized network of decision makers. Consequently, the Army must be able to adequately defend the networks it depends on for C2 and ISR. To do this, it must understand how its information moves through the cyber environment. Similarly, the Army must be able to understand and therefore to exploit adversarial cyber networks.

The Army depends on a robust C4ISR capability to sense its environment and then make sense of that environment. Sensing the environment involves the employment of ISR assets (the Sense function). C2 tools and processes are then used by decision makers to make sense of that environment and then to share knowledge, situational understanding and command intent and direction (the Command function). What enables both functions, and ultimately links Command and Sense together, is the cyber environment.

Collectively, then, the Command and Sense functions are wholly described by C4ISR: C2, computers and communications (cyber), and ISR. As the glue that keeps the operational functions together, the network is an indispensable enabler of Army operations. Put simply, the Army cannot fight without it, and that implies an absolute requirement to defend it. Conversely, if the adversary depends on its network to fight, then the Army should be able to deny the

adversary that ability. The relationship between cyber and C4ISR is described in more detail in Annex B to this chapter.

There are many network threats which the Army must defend against. Firstly, there is the threat posed by friendly action (or inaction). That threat includes unintentional actions, such as changing hardware or software configurations for the perceived good of one part of the network, which in turn unintentionally undermines the effectiveness of another part of the network. It also includes malicious insiders and the WikiLeaks phenomenon. Threats posed by friendly action can usually be countered through existing techniques of IS security (including procedural security, personnel security and configuration management) and network hygiene practices. Secondly, the cyber defence must concern itself with neutralizing the actions, or the effects of those actions, taken by adversarial actors conducting operations in the cyber environment. Cyber threats posed by adversarial action range from individual Internet nuisances to nation-states either exploiting national capabilities or work through nefarious third-party contractors. Defeating that type of threat requires the traditional military and non-military capabilities of the nation, as well as new capabilities wholly exercised within the cyber environment.

In order to defeat the effects of adversarial actions within the cyber environment, the Army will need to possess the capability to understand what actually happens within the cyber environment. With sufficient situational awareness, the Army will be able to intelligently defend the components of cyber that it relies on for mission assurance. Such situational awareness will also inform the rapid development of alternate and contingency plans which further guarantee mission assurance. To exploit cyber SA in the development of intelligent defences, the Army will need to possess the requisite hardware and software components, combined with expert knowledge, which will allow it to shape and defend its vital cyber ground. Commanders must understand the vulnerability of the cyber environment and its impact on land operations. To know how to operate effectively within the cyber environment, they will rely on specialists who are capable of rapid and decisive cyber manoeuvre.

The conduct of a defence in cyber cannot be directly compared to an area or mobile defence as described in existing land operations doctrine. As opposed to these traditional land concepts, the ability to shape and re-shape the cyber environment makes “holding ground” or “destruction of the enemy” options of last resort. In the cyber environment, ground may be given up if it can be

re-created elsewhere. In a similar fashion, rather than destroying the enemy, the Army can observe the enemy, who may reveal their intentions for future action in other environments. While observing the enemy, the Army can simultaneously manoeuvre around them, taking advantage of other spaces within the cyber environment.

There are three ways to defeat an enemy in the cyber environment: defeat their electronic activity within the friendly cyber area of operations (i.e., the Cyber AO) through defensive counter-moves; defeat them electronically in their own battlespace within the cyber environment through offensive cyber operations; or defeat their cyber operators and cyber infrastructure through operations conducted in a different physical environment—land, aerospace, or maritime. Possessing the capability to exploit and attack adversarial networks makes a great deal of sense in many contexts. In others, it may undermine operational objectives. In short, offensive capabilities in the cyber environment must be governed by the same type of policy framework that governs offensive operations in the other physical environments.

For the same reason the Army would not want to bomb a hospital, it would not want to manipulate the cyber environment in such a way that a hospital's power supply is wiped out by an unintended downstream effect. If an offensive cyber operation is launched against a legitimate military target, it must be considered as being no different than a traditional EW operation and would follow appropriate rules of engagement (ROE) and national policies.

Failure to develop cyber operations capability in the Army must be considered high risk. As the Army moves forward in its transition to the Army of Tomorrow, the network will become the key enabler of success. The Army's vision of conducting full-spectrum operations in the manner prescribed by ADO is unachievable without the network glue holding operations together. Assuming that the network will be there in the absence of a thoughtful defensive capability represents an unacceptable risk. Moreover, defeating the adversary by denying them or exploiting the use of their own networks is potentially a war-winning capability, with a close relative in existing EW doctrine, and represents an option well worth considering.

In order to successfully defend its overarching C4ISR system, the Army must have the capability to effectively sense those regions and components within the cyber environment upon which it relies for freedom of manoeuvre. It must have the personnel, technology, training, and processes in place to ensure an

intelligent and responsive cyber defence, which in turn enables operational success and sets the conditions for the conduct of other cyber operations, such as offensive activities against the adversarial Cyber AO—to include exploitation and attack (Note – exploitation and attack do not necessarily mean CNE and CNA, but can mean ES, EA, other tactical activities, or combinations thereof). CNO must be integrated with EW in order to exploit technological convergence and existing synergies between the two mission sets. The Army must transition away from static information assurance models toward the conduct of integrated cyber operations that deliver mission assurance.

Inside the cyber environment, the Army requires a battlespace framework akin to the one described in existing land operations doctrine. Specifically, areas of interest (AIs), areas of influence (A of I), and areas of operations (AOs) must be described and understood.

Although the AO is explicitly defined by the commander's superior, the commander has to make his or her own assessment in order to identify his or her AI and A of I. A commander's Cyber AO will therefore likely consist of CAF networks only, for superiors will have no ownership of communications and computer network infrastructure beyond their Operational Authority. These networks include the hardware and software components of all computer and communications networks and all manner of cabling and EM spectra in between. The AI will be defined by all of those things that can influence the commander's AO, and will include JIMP, local, and adversarial networks and network infrastructure, the electromagnetic spectrum, and all electronic devices capable of manipulating the cyber environment within the commander's geographic AO. Finally, the commander's A of I must consist of the AO and certain aspects of the AI as determined through the estimate process. The commander must understand all aspects of his or her physical environment and how they interrelate, including cyber. He or she must understand how his or her actions in the cyber environment can affect his or her own processes and systems, those of JIMP partners and, of course, those of the adversary. It all begins with a commander understanding the makeup of his or her own Cyber AO and recognizing the need to defend it.

4.4 COMPUTER NETWORK DEFENCE AND THE CYBER PICTURE

Land operations must be continuously fed by information. Timely and relevant information ensures that decision makers—from commanders and staff in headquarters through to dispersed force elements in the field—can

develop workable options and make the right choices in determining the optimal way of influencing the battlespace. Information is obtained through ISR systems and managed through the intelligence process. ISR systems sense the environment using a variety of sensor systems, including EM. Once it has sensed, the system must then do one of two things. It can process raw data onboard and send its processed information to a decision maker, or it can convert the sensor input into an electronic signal to pass back to another system component capable of conducting the requisite analysis. From there, information ultimately still must be passed to a decision maker. In other words, all ISR sensors must be part of the overarching C4ISR network; they are rendered ineffective if not properly networked. ISR sensor networks are therefore the first component of our Cyber AO that must be defended.

ISR sensor networks are vulnerable to myriad electronic threats, including those already extensively detailed in existing EW doctrine such as spoofing, hacking, and jamming. The adversary can adopt any number of techniques to defeat a sensor, including disruption of the sensing payload itself, the software or hardware components of the sensor's onboard processing components, its communications systems, or even the actual data stored on the sensor network. Because ISR networks are in turn networked with C2 capabilities (forming the overarching C4ISR architecture), the C2 function is also susceptible to disruption or degradation resulting from adversarial exploitation of the ISR system. ISR systems feed information to decision makers, who in turn rely heavily upon cyber infrastructure to process information, conduct operational planning, deliver orders and perform battle management tasks. In addition to the link between ISR and C2 systems, our command and control systems are also linked to other agencies and Allied partners. In the domain of computer networks, there is an adage that one poorly secured network introduces risk to all the networks it connects to. An adjoining Allied flank on the battlefield adds robustness and strength, but in the cyber environment it almost certainly introduces vulnerability. Computer networks and communications systems constituting the Cyber AO must be defended from all conceivable avenues of approach to ensure freedom of manoeuvre for the passage of friendly information and to preserve the integrity of friendly information itself.

The adversary has many techniques to interfere with the Army's Cyber AO. Although many such techniques remain steadfastly within the classified purview of the intelligence community, some generalities may be commented on here. Wireless links are susceptible to jamming, blocking, and infiltration.

Wired connections can be physically cut or attacked using EMP-type weapons designed to manipulate electron flows. All network equipment (including infrastructure and terminal devices) is susceptible to EM attack, which can manipulate electron flows, damage electronic parts, and degrade information stored on electromagnetic media. It is also susceptible to adversarial computer network attack, which, much like electronic support and attack techniques, includes jamming (buffer overflow; denial of service such as ping floods and teardrop attacks), spoofing (packet spoofing, cross site scripting, DNS hijacking, password cracking), electronic eavesdropping (Trojan horses, backdoors, keystroke loggers, screen capturing tools, packet sniffers), and physical destruction (malicious code such as worms and viruses).

In order to understand what the adversary is doing on our networks, the Army requires the capability to see and understand its own Cyber AO. The personnel, tools, and techniques required to gain such understanding must be put together in such a way as to generate an easily explainable Cyber Picture which differentiates friendly activities from potential adversarial effects. The picture would show what an adversary is doing and allow cyber staff to discern the adversary's capabilities and intent. (There are several software applications which allow for the development and maintenance of a Cyber COP, but well before adopting any such tool, a full PRICIE+G analysis would have to be conducted to ensure the appropriate degree of action and interaction between artificially intelligent entities and cyber operators.) Armed with such intelligence information, commanders and staff can develop meaningful plans to thwart the adversary and, if required, counter-exploit or counter-attack (using cyber techniques, other means, or combinations thereof). This is no easy task. As William J. Lynn III (Deputy Director of Defense, US Department of Defense) recently said in an interview with *Frontline Security*:

In the cyber arena, knowing who your adversary is, and what they've done, is a key part of mounting an effective response. Yet determining where an intrusion originates from, and who is responsible, are among the most difficult challenges we face.⁴⁴⁵

The Cyber COP need not be simply a live map of the Cyber AO. The digital tools and techniques which allow for the development of a Cyber COP within

445. Clive Addy, "An Urgency for Cyber Security Leadership" in *Frontline Summer* 2010, 9.

the Cyber AO may equally be applied to the Cyber A of I (which, as already mentioned, ideally includes the Cyber AI). Techniques used to neutralize adversarial actors, or the effects of their actions, within the Cyber AO may likewise be extended to the Cyber A of I. Although technically possible, and potentially offering a war-winning capability against a network-enabled adversary, such extension of cyber operations beyond the friendly Cyber AO must be first and foremost grounded in clearly articulated GoC policy. It should be noted that such policy will likely not be developed quickly. That is because the problem is not as simple as developing policy for the use of conventional weapons with relatively limited areas of influence. The use of a cyber technique on an adversarial network may have unintended downstream consequences which could undermine operational objectives in ways that political and technical communities alike do not yet understand. As a United States general once remarked when talking about neutralizing the French-engineered Iraqi AD system during the First Gulf War, a cyber option was considered but rejected over fears that such a technique might knock out all the ATMs in Paris.

The bottom line is that the Army requires the capability to see, understand, and defend its network. Such a capability will ensure the continued operation of the Army's critically important C4ISR system. Furthermore, should the opportunity present itself, the Army must have access to capabilities that permit the rapid defeat of network-enabled adversaries. Such capabilities may include the techniques of cyber exploitation and offensive cyber operations and will require a clearly defined policy framework.

An effective Cyber Defence must be robust and layered in order to ensure protection from adversarial intrusion, exploitation/intelligence collection, and attack. There are many options for the defence: how to configure it, with which tools and techniques, in which organizations, and with what balance of humans, machines, and code. There are also options for augmenting the defence with exploitative or even offensive capabilities. An important consideration will be whether the Army should seek to own a particular capability, or merely ensure that it has an acceptable degree of access to a CAF or Allied capability. Perhaps a mix of all these things will best ensure effectiveness, redundancy, an acceptable balance of risks, and affordability. In any event, while attack and exploit capabilities can certainly enable ADO, it is the network that will underpin ADO. The Army must therefore invest in a cyber defence capability. More detail on possible options can be found in the PRICIE+G analysis found in Annex A to this chapter.

4.5 CYBER AND THE OPERATIONAL FUNCTIONS

Command is inherently a human endeavour. However, the Command function cannot be exercised effectively in land operations without an underlying network to hold it together. The cyber environment is essential to a commander's exercise of C2 and must be defended much like any other piece of vital ground. Execution of the cyber defence requires a mix of humans and machines. Automated cyber tools are as able to neutralize threats and exploit opportunities as their human programmers allow them to be. However, there is ultimately no degree of software autonomy high enough to negate the requirement for human decision making in this environment. Maintaining an effective defensive posture and overseeing personnel and materiel in countering threats to the integrity of information and infrastructure within the Cyber AO requires a significant degree of experience, training, creativity, and cognitive ability. It requires the authority and the ability to make decisions quickly and fully understand the consequences of those decisions. It is not an environment to be managed. Cyber operations must be commanded. Cyber is the glue which holds ADO together: responding to threats to cyber must not be a function of policy and bureaucratic management. Although staff may be able to inject cyber options into a commander's tactical plan, the execution of such an enabling cyber operation must be led by a commander. Manoeuvring in the cyber environment can expose an adversary to defeat in an instant, and can similarly undermine friendly land manoeuvre. That responsibility must be entrusted to be a commander who intimately understands the cyber environment and its potential effects on land operations.

Sense is executed via the ISR function, which is wholly dependent on an underlying network of sensors and processors (both electronic and human) ensuring the passage of timely and relevant information to decision makers. To manoeuvre in the cyber environment, whether neutralizing a threat or exploiting a vulnerability, a high degree of situational awareness about the environment and how everything fits together is required. As in the other physical environments, the Sense function involves more than just compiling data. It includes analyzing data with a view to gaining sufficient situational understanding to develop COAs for manipulating (influencing) the environment in a way that enables mission success. Knowing what to look for in an adversarial network is as important as understanding what your own Cyber AO looks like from an outside perspective. Only with a true understanding of the cyber environment can appropriate action be taken to shape and re-shape it in one's favour.

Act includes all actions taken by military forces to influence their environment. Actions are preceded by decisions. Decisions are made after the conduct of an estimate which is fed by operational information. This planning process, at every level, depends on the availability of information and, therefore, on the network. Like the other operational functions, Act is heavily dependent on the cyber environment. Within cyber itself, activities can be conducted which are decisive. Networks (and elements depending on network control for continued functionality) can be physically destroyed simply through electronic manoeuvre. A jammer can defeat a UAV's command links and send it crashing to the ground. A computer virus can neutralize a main battle tank's fire control systems and render it combat-ineffective. Such actions can only be taken when policy supports their use and collateral damage can be estimated with sufficient precision. The DRDC CORA paper *Understanding Cyber Operations in a Canadian Strategic Context: More Than C4ISR, More Than CNO* (Bernier and Treurniet, 2009) presents an excellent analysis of cyber operations using the operational function framework. It includes some relevant options for engaging an enemy in the cyber environment:

- Create a virtual diversion to occupy the focus of the enemy command and control.
- Degrade the network-based communications systems of the enemy.
- Deny a secure communications service so that unencrypted communications must be used.
- Modify information in the cyber portion of the enemy command and control systems to mislead them into, or keep them in, a vulnerable position.
- Insert false information on a friendly system in order to allow the enemy to find it during an enemy reconnaissance activity.
- Penetrate and gain control of an enemy's weapon system and use the system against it.⁴⁴⁶

Note that Bernier and Treurniet assume that effects in the cyber environment can be generated only through the use of CNA.

446. Melanie Bernier and Joanne Treurniet, "Understanding Cyber Operations in a Canadian Strategic Context: More than C4ISR, More than CNO," in *2010 Conference Proceedings*, ed. Christian Czosseck and Karlis Podins (CCD COE Publications, May 2011): 234.

The cyber environment can shield the Army and in turn must be shielded. The ability to operate in the cyber environment to counter adversarial electronic or computer network attack adds to the Army's omni-dimensional shield, protecting soldiers, equipment, and infrastructure. Because the cyber AO is human-made, it is highly susceptible to adversarial human influences. In this environment, an adversary can re-shape the Army's AO, while simultaneously feeding false information into Army ISR systems which indicate that nothing has changed. Specialized tools, training, and understanding will be required to properly shield cyber infrastructure.

The cyber environment can enable Army sustainment, and in turn it must be sustained. The future ADO enabling concept of focused logistics is centred on the availability of the network and its HW/SW components at every layer. Therefore, the cyber environment will continue to be a key enabler of the Sustain function. Conversely, the Cyber AO itself needs to be sustained. To enable responsive defences and maintain the initiative for other cyber activities, the Army will need access to the latest technologies, without being constrained by glacially paced procurement policies and procedures.

4.6 RISK AREAS

There are a number of factors that may hamper the cyber capability development process. They include, but are not limited to, the following:

- Effective sharing of cyber information is crippled by security caveats, the technical nature of cyber, and legal and privacy issues.
- Risk homeostasis and a lack of true cyber SA have contributed to inaction in the strategy and policy domains.
- Supply chain security for both hardware and software needs to be addressed, but no one has figured out how to tackle it yet.
- The cyber threat is growing ever more sophisticated, and access to almost any network is becoming relatively simple. Therefore, the goal for cyber capability developers should be mission assurance (through business continuity planning) as opposed to network assurance (which is probably a nearly impossible task).

- Cyber personnel are considered high-demand, low-density (HD-LD) human resources. Therefore, tailored personnel strategies must be developed for recruitment, training, and retention.
- There is a need for good cyber policy enforced by knowledgeable and tech-savvy leaders.

PART FIVE – CONCLUSION AND QUESTIONS

In summary, the Army requires assured freedom of manoeuvre in the Cyber AO, which in turn requires robust protection and preservation of the ANE (which includes the EMS). The Army lacks situational awareness (SA) of its own network environment. Without this SA, it cannot adequately defend the ANE. The tools required to gain SA and repel threats, when combined with existing EW doctrine and capability, enable cyber defence and lend themselves well to potential use against network-enabled adversaries. Freedom of manoeuvre is only possible through the maintenance of a dynamic cyber defence capability, which must include ISR and powerful countermeasures. Deploying a static network capability that continues to delink CIS from EW and CNO will create the conditions for command paralysis and subsequent mission failure.

The next step in the capability development process for Future Army Cyber Capability (FACC) is for the Army capability development community to discuss the concepts described in this paper. Specifically, these concepts include the conceptual definition of the cyber environment (the convergence of CIS, EW/SIGINT, and CNO domains—i.e., the EM battlespace), an acknowledgement of the cyber deterrence problem, the potential utility of offensive cyber operations, the requirement for a cyberspace framework—akin to the battlespace framework—which supports the development of cyber situational awareness and a cyber picture, and a recognition of the need for a computer network defence capability as distinct from IS security and network hygiene tools and procedures. The Army capability development community cannot wait for policy direction in order to determine how it fits into the larger defence picture. In the absence of clear policy, the Army can contribute to the development of such policy by clearly articulating exactly what it wishes to achieve in the cyber environment. Arriving at such an articulation is no small task, but it must be done so that the Army can make the most informed decisions possible as it transitions beyond F2013 into a network-enabled force truly capable of conducting ADO.

To reach consensus on the FACC, it would be worthwhile for the Army to consider conducting a seminar wargame in order to help answer the following questions:

- What are the boundaries of the cyber environment? A clear answer to this question is essential because it will enable the Army to fully understand its vulnerabilities and those of its adversaries.

- What would the Army like to be able to do in the cyber environment?
 - » If it wishes to defend, what exactly does it need to defend against? Which systems must be defended? What are the options?

 - » If it wishes to collect intelligence or conduct an offensive operation, what sorts of targets is it realistically interested in? What are the options?

- What are the costs (PRICIE+G) associated with operating in this environment?



Source: Combat Camera

ANNEX A – PRELIMINARY PRICIE+G ANALYSIS

PERSONNEL AND LEADERSHIP

The cyber environment is defined as the component of the physical plane that involves the manipulation of electrons with electromagnetic energy. It follows that the Communications and Electronics (C&E) Branch would continue to provide the bulk of CAF personnel dedicated to manoeuvring within this environment. Cyber is currently regarded as a contested battlespace because it is a shared space, and therefore friendly force freedom of manoeuvre cannot be guaranteed. For mission assurance, the CAF relies heavily on its Information Operations Group (CAFI OG). A source of training, professional development, and experience building in the cyber environment for Army soldiers, CAFI OG concerns itself with defence of strategic networks and the strategic protection and exploitation of the EM spectrum. As a capability that is so intimately tied to intelligence, and sits so firmly within the JIMP context, cyber capability must be centrally managed and, in many circumstances, kept at the SECRET level or beyond. That said, different CAF organizations will have different Cyber AOs. That in turn implies that those who are responsible for a unique Cyber AO must have the capability to protect and influence that AO. For the Army to ensure its own cyber defence, it will need to assign forces accordingly (this will be discussed further in the section below focusing on organizational impacts). Options analysis will have to take place during future CD efforts to determine where service interests sit in terms of conducting cyber activities beyond service-specific AOs.

There is a clear requirement for leadership at all rank levels within the cyber environment. In order to quickly and accurately determine whether a particular electronic event or information anomaly comes from an adversarial source or has a particular electronic signature, cyber operators must possess a high degree of professional competence. Competency can either be trained through formal education or developed through hands-on relevant experience. Both methods require a significant time investment. In a cyber operations centre, where a decision must be made on a course of action based on the presence of a threat, leadership must come not only from the senior rank present. All operators must be prepared to assert themselves when there is ambiguity over the nature of the threat or the best way forward. In the cyber environment, because it is largely a technical and human-made environment, a private signalman may well know the best way forward while a lieutenant-colonel may be at a loss. In other circumstances the reverse will be true. In all

circumstances, decision making by officers in command must be shaped by input from across the cyber operations team. Flexibility in leadership models has to be an organizational principle for cyber elements. How much flexibility is desirable is best determined through a combination of operational experience, Allied engagement, experimentation, as recently exemplified at the CAFSCE Cyber Challenge, and wargaming by senior leadership (as required).

Antiquated notions of branch succession planning that aim to move operators in and out of operational and support roles and across the various electronic battlespace domains will only serve to marginalize the true potential of the personnel component of Army cyber capability. Although cross-training and a wide breadth of experience may be beneficial for some C&E positions, that is not true for domains that require deep specialization. Force Generation (FG) takes time, and CAFIOG and the Army presently battle the demands of the Branch to move trained EW and CNO operators into other CIS-focused domains (e.g., brigade units, garrison support units, cryptologic or engineering units, ADM(IM) or the operational commands). Succession planners must be adept at balancing the requirement for breadth of experience with the demand for deep specialization required by the cyber domain.

The CAF currently has one unit dedicated to CNO. The CF Network Operations Centre (CFNOC) is the organization within CAFIOG charged with the exclusive CNO mandate. It currently has VCDS Manning Priority 2 status, which, according to the VCDS website, applies to units that conduct critical sustaining and change activities, defined as activities which are “fundamental to enhancing future operational effectiveness and distinctive competencies while sustaining the current operational tempo.” It follows that any unit involved in the FE of cyber forces would be assigned VCDS Manning Priority 2.

**RESEARCH AND DEVELOPMENT AND OPERATIONAL RESEARCH
(PLUS EXPERIMENTATION)**

The C4ISR Research Program, which includes R&D relating to the cyber environment, is managed under Client Group 5.

The C4ISR R&D program supports the joint and national-level commander and staff in fulfilling the roles outlined by the Defence Planning, Reporting, and Accountability Structure (PRAS). Its scope includes work on communications, information and knowledge management, information

architecture and information technology, information operations, national-level and joint command and control, surveillance, intelligence, and space.

The following thrusts are included under the C4ISR program: 15a (Command and Control); 15b (Communications and Network Operations); 15d (Intelligence); and 15e (Space Systems and Technologies for Defence Applications). Projects applicable to cyber under these thrusts include Multi-core Monitoring and Soft Redundancy for Cyber Attacks Resistance; Computer Network Defence Decision Making; Securing Information in Coalition Operations; Communications in the North; Scoping Study: Cyber Attack Protection; Advanced Computer Security Incident Inv'n [*sic*], Modelling and Simulation of Cyber Effects and Capabilities for C2; Adaptive Spectrum Utilization for Assured Communications; Security & Trust in Dynamic Ad-Hoc Networks; Advanced Studies; Cyber Incident Integrated Rapid Response; Cyber Attack Protection of DND/CAF Info Sys; Automated Network Defence (ARMOUR) TD; SAMSON TD; and Flexible Communications—Satellite Payload TD. Once the Army has determined its future course for cyber capability development, this list of projects will have to be examined in detail to determine whether S&T gaps exist and, if so, close gaps or assume risk.

Cyber operations are one of the focus areas of the CORA Joint Systems Analysis Section. This statement appears on its website:

In the Canadian Forces, cyber operations are currently considered to be primarily computer network operations (CNO), where CNO is categorized as a subset of C4ISR, providing support to operations in the physical environments. To use these capabilities to the fullest extent, arguably an integrated operational environment is required, and thus the current CNO model, comprised of three separate activities (computer network attack, computer network defence and computer network exploitation), should be abandoned in favour of an integrated model of cyber operations. Scientists in the JCOR section have analysed cyber operations in terms of the CAF's six functional domains: Command, Sense, Act, Shield, Sustain, and Generate and have concluded that cyber strategies should be developed by looking at the full spectrum of cyber operations rather than focussing solely on CNO to ensure that all cyber effects are considered.⁴⁴⁷

447. DRDC CORA – Joint and Common, "Cyber Operations," last modified 21 March 2012, <http://cora.mil.ca/jcOR.asp#drdcpart02>.

The US military (including the wider defence community) is currently conducting extensive R&D into cyber operations. Significant recent activities include the construction of a Joint IO Range and ARCYBER's hosting of a Cyber Summit. There will be information coming from USCYBERCOM CAFLO LCol B.C. Mosher on the results of the Summit, specifically how R&D and Experimentation have supported the US Army's cyber options analysis. The use of cyber ranges and LVC environments by Allies should be examined in order to inform the development of modelling and simulation options for the CAF.

INFRASTRUCTURE, ENVIRONMENT, AND ORGANIZATION

The Army Network Operations Centre (ANOC) is an organization within DLCI responsible for the Operational Control, Technical Control, System Support, and IS Security of the Army Network Environment (ANE). The ANE includes LCSS and Army-apportioned instances of national networks (e.g., CSNI, DWAN). The ANOC relies on a network of ISSOs (in the future, there will be CND Teams) for reach into Army units and formations. For deployed operations, the ANOC envisions having similar reach. This raises a number of organizational questions about the defence of deployed Army networks, such as the following:

- Should the ANOC be the central hub for deployed Army networks? If so, does it oversee the network defence? Does it conduct the defence exclusively (with deployed forces responsible for routine IS Security practices)?
- Should deployed LCCs plug into coalition NOCs or the ANOC? Which is the priority? Is it different for a deployed JTF?
- What is the lowest organizational level that would require a cyber picture or COP? Should a forward ANOC be deployed with certain mission packages? Should a JTF J6 be able to see into his or her networks? What about a unit ISSO? If so, are these the only people that would need this kind of cyber visibility? Who would need access to a cyber picture?

Domestically, OGDs (specifically Public Safety and CSEC) have the lead for cyber activities conducted on behalf of the Canadian government—including the defence of government networks. DND maintains responsibility for defence

of its own networks only. On international operations, the Army is responsible for protecting and defending its own electronic networks so that freedom of manoeuvre and information confidentiality, integrity, and availability (CIA) can be assured. (Networks include not only computer networks and their information and software, but also the EM spectrum and its associated electronic devices such as radios and telephones.) In the past, protection of networks was simply a matter of obeying standards and ensuring proper configuration management. The possibility of an active threat operating within the Cyber AO will require a robust CND posture augmented by appropriate network ISR capabilities. A layered network defence, from deployed operators all the way back to the ANOC, likely makes the most sense, although such a conclusion must of course be further evaluated through experimentation, operational research, and discussion with joint and Allied partners.

Should the Army find itself fighting a network-enabled adversary, significant advantage may be gained by possessing the capability to deny the enemy the use of their networks. If the tactical plan can be better supported by exploiting the adversarial network environment (e.g., rather than using fires to destroy network infrastructure, the same result could be achieved by electronically manipulating the information residing on adversarial networks), then the Army should have the capability to do that as well. The doctrinal overlap here with EW is obvious. EW is not simply a matter of electronic attack. It includes all manner of electronic information collection, processing, and exploitation in order to deny the adversary the effective use of their electronic communications systems. EW can be greatly enhanced by CNO techniques, just as CNO can be enhanced by borrowing from the doctrine and best practices of EW. Electronic convergence makes it difficult to maintain organizational separation between EW and CNO force elements.

The Army does not have integral CNO elements, but it does have its own EW capabilities and organizations. Electronic convergence seems to point to the EWCC as a potential focal point for the coordination of Army CNO activities pertaining to adversarial networking capability. Re-organizing, training, and equipping EW force elements as cyber force elements makes sense for the creation of optimal electronic synergy in the exploitation of the adversary. It also makes a great deal of sense for cyber force elements to be engaged with network defence. The overlap in the tools required for gaining network SA and the doctrinal fit with the larger intelligence community (in understanding adversarial tactics and signatures) seems to imply that cyber defence rests more logically with the EW/SIGINT community than the CIS community. In

addition, the ability to neutralize a threat fits within the Act function, suggesting that such neutralization ought to be coordinated by the EWCC—an entity already organized, trained, and equipped for planning and coordinating electronic support and attack. If network analysis reveals a vulnerability in the Cyber AO, then the cyber force element can inform the CIS network managers to take appropriate action. This would be similar to a MEWT commander telling a J6 to abandon a certain frequency band or encryption posture because of the presence of an adversarial threat. The MEWT commander does not own the spectrum but is best positioned to understand who is using elements of the spectrum and for what purpose. This is wholly analogous to CNO. EW and CNO, enabled by SIGINT, work together to enable CIS.

CONCEPTS AND DOCTRINE

The Army's future cyber concept is heavily focused on the convergence of three network operations domains: CNO, EW, and SIGINT. Therefore it makes little sense to say that the Army will focus on CND exclusively and let government policy makers and higher CAF formations think about CD activities pertaining to concepts involving CNA and CNE. The three CNO activities are inextricably linked, just as they are linked with the EW activities of EP, EA, and ES.

The Army needs a robust cyber defence (enabled by EP). It must therefore be capable of conducting ISR within its own networks and countering threats within in its own networks. ISR tools used in the friendly Cyber AO can be used beyond it; counter-attack tools may just as easily be employed in a pre-emptive role. In other words, such defensive capabilities readily extrapolate themselves to exploitation and attack of adversarial networks. Such thinking is not new ground for the Army. TTPs associated with CNE and CNA are linked to those associated with ES and EA respectively. There is great fear of the unknown in the political-legal domain when it comes to cyber warfare. To be sure, the Army would not risk the destruction of critical civilian infrastructure while conducting its cyber operations in the future, any more than it would take such risks when firing an artillery round. However, against a network-enabled adversary, the disabling of the adversary's critical battle command systems can be a war-winning capability.

A number of doctrine publications will require updates once the Army has answered the questions outlined in Part Five above. These include, but are not

limited to, *Land Operations*, *Electronic Warfare*, and *Signals in Land Operations* (all volumes). A doctrine update would be required to define the cyber environment and its relevance to land operations and clearly outline the associated activities that Army organizations will be expected to conduct. Roles of specific units, including any changes to organizational structures, must also be articulated in appropriate doctrine.

Battle task standards (BTSs) are currently undefined for the cyber environment. An update would be required to *BTS for Signals* (Directorate of Army Training's Approved Battle Task Standards List, Chapter 5).

INFORMATION MANAGEMENT AND TECHNOLOGY

This component of the PRICIE+G analysis relates to how other capabilities influence and are influenced by IS/IM/IT. It is explained in the essays above. In short, information systems and architecture compose the physical infrastructure of the cyber environment. The future cyber environment will eschew former notions of IS Security and static configuration management models and will be characterized by rapidly changing architectures (including supporting systems and their components) which enable cyber manoeuvre while facilitating the timely neutralization of adversarial threats.

EQUIPMENT AND SUPPORT

There are several unique considerations for equipping forces that operate in the cyber environment. First and foremost, of the five physical environments, it is cyber that is considered the technical environment. It is technical because it is a human-made environment (including human-made electronic devices which manipulate the EMS component of the environment). Mission success depends on guaranteed freedom of manoeuvre, which in turn depends on having the newest technology. The Cyber AO will always be susceptible to a zero-day attack; newer tools and techniques will always find new vulnerabilities and be capable of new exploits. However, those operating in the Cyber AO who are equipped with the latest technologies will have the clear advantage. Thus, there is an absolute requirement for rapidly responsive procurement strategies and robust supporting R&D (including experimentation). Management strategies should correspond to existing Army processes for computer network, EW, CIS, and supporting equipment. Supporting systems for the cyber environment include all systems composing the Army C4ISR environment.


Environmental concerns pertain to the survivability of network infrastructure, including EMS (critical) and edge devices (less critical). There is no requirement for the Cyber AO to be indestructible and/or impenetrable. Such goals would be unachievable. The capability goal is simply to ensure freedom of manoeuvre within the environment. That may require the abandonment of certain parts of a contaminated network and the flexibility to expand the network away from a threatened sector—even potentially into the adversarial Cyber AO.

GENERATE

Professional development (PD) is required for those less versed in technical aspects so that they can understand the makeup of the cyber environment and how it can enable land operations for the better or, conversely, influence those same operations for the worse. PD opportunities exist with Allies and through CAF organizations such as DG Cyber and CAFIOG. Canadian universities and OGDs provide another venue for PD for both the command support and operator communities.

Individual training will be required for all those who conduct operations within the cyber environment. Such specialist training cannot occur within unit lines. It will therefore have to take place at institutions like CAFSCE or with Allied or other trusted external organizations. Many courses offered at CAFSCE already have application to the cyber environment. Some examples are *ATCCIS*, *ASP*, *JCCIS*, *Communications Research – QL3*, *QL5*, and *QL6A*, *EW Land Basic*, *Operational SIGINT Analysis*, *EW Land – Support to Operations*, *SIGINT Officer (Basic)*, *CF Cyber Operations Staff Officer Course*, *Canadian Forces Network Operations*, and *Network Defence Analyst*. Training plans for those courses may be reviewed and revised, and there is always the possibility of introducing new specialist courses, similar to CAFSCE’s recent work standing up the aforementioned *Cyber Staff Officer Course* and the *Network Defence Analyst* course.

Two types of collective training (CT) are relevant in this analysis. The first is CT among cyber specialists. Such training would occur in simulated environments and endeavour to develop, maintain, and/or confirm cyber TTPs within (and between) cyber teams. CAFSCE’s Cyber Challenge is an example of the type of exercise that can be run for deep specialists (albeit with expansion of exercise objectives to include confirmation of relevant BTSs). Specialist CT cannot occur on live networks. That further substantiates the requirement for construction and maintenance of so-called cyber ranges



(closed internal networks), where various cyber techniques can be test-fired without risking harm to real-world infrastructure. In addition, cyber CT must be integrated with traditional land exercises. For incorporation of cyber operations into a CAX environment, it must be determined whether existing simulation tools within the Army Simulation Centres (ASCs) are capable of modelling cyber (CNO and EW) effects. If not, there are many types of simulation tools available that can, and their interoperability with existing ASC infrastructure should be investigated. When incorporating cyber operations into field training exercises, special care must be taken to ensure that the effects of CNO or EW activities do not cause unintended effects on local or surrounding infrastructures. Exercise planners must also strive to find the right balance, incorporating cyber effects without crippling an overall training event.

ANNEX B – CYBER AND C4ISR

This annex will present several visual aids to help articulate the relationship between cyber and C4ISR. The C2 process describes the Comd function, while the ISR process describes the Sense function. Both processes are heavily dependent on underlying communications and electronic systems (communications and computers) which, when networked together, inextricably link the Command and Sense architecture. C4ISR therefore describes the convergence between the Command and Sense operational functions.

On the other hand, cyber is defined as the environment where computer network operations (CNO) are conducted. It is a rapidly expanding environment thanks to technological convergence, which continues to blur the lines between the network operations domains of CIS, CNO, SIGINT, and EW. The link from cyber to the Command and Sense operational functions is obvious. However, as shown in Figure 5.B.1, cyber also encompasses aspects of the cyber-electromagnetic environment that extends well beyond regions controlled by friendly forces. C4ISR, on the other hand, extends beyond the physical cyber-EM environment of friendly forces to include other aspects of friendly ISR along with the cognitive aspects of C2.

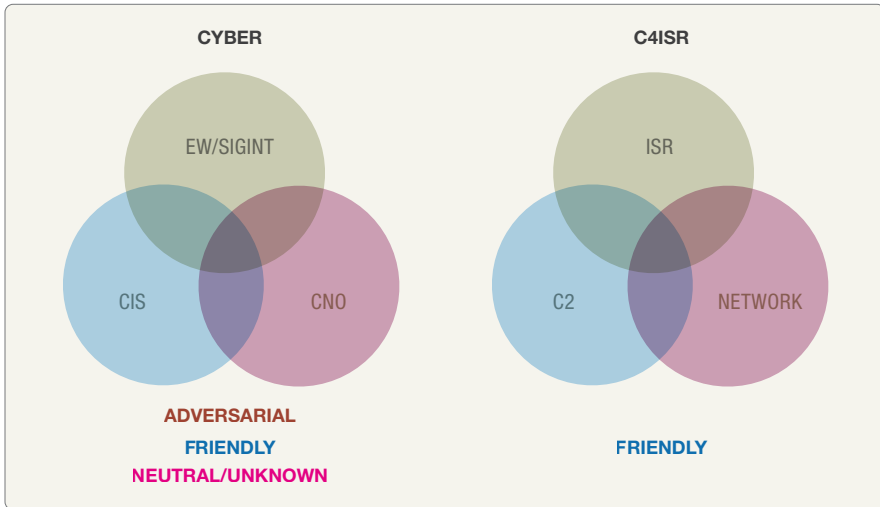


Figure 5.B.1: Cyber and C4ISR

In Figure 5.B.1, the differences and commonalities of cyber and C4ISR may not be obvious. Figure 5.B.2 attempts to add clarity by depicting the land operating environment as a simplified puzzle.

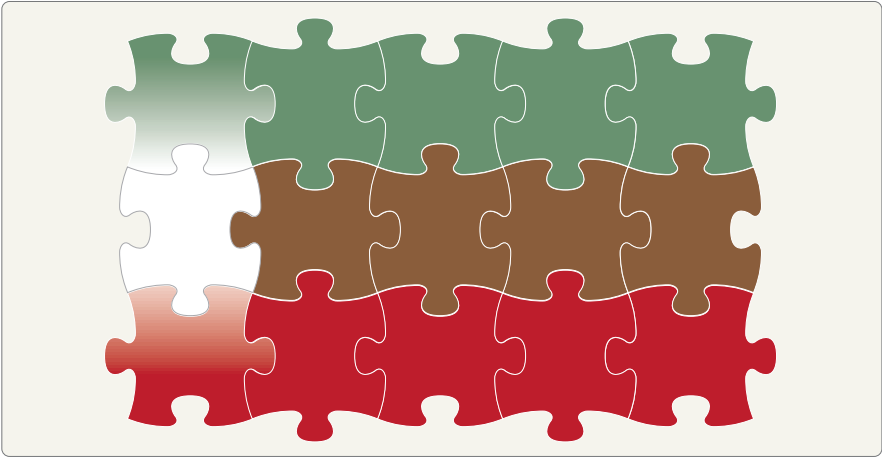


Figure 5.B.2: The Land Operating Environment

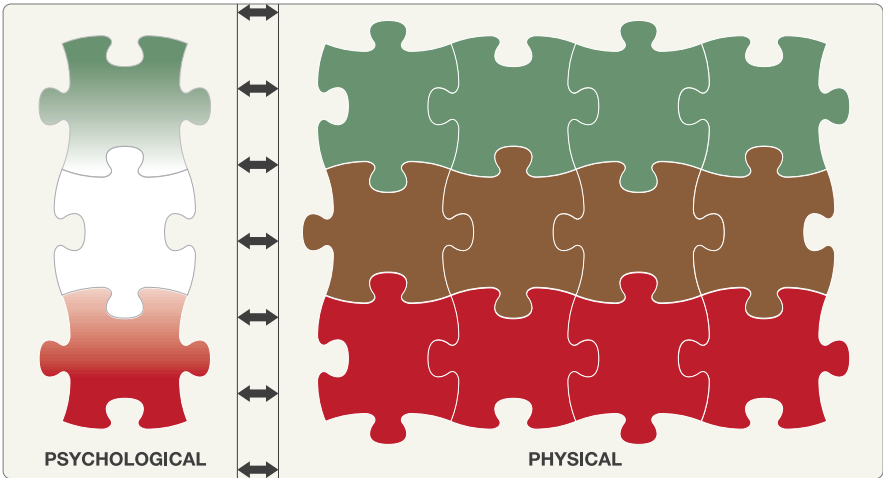


Figure 5.B.3: The Physical and Psychological Planes

Figures 5.B.2 and 5.B.3 show how the land operating environment breaks down into a combination of friendly (coded in green), neutral (coded in brown and all white), and adversarial (coded in red) actors each occupying the physical and psychological planes.

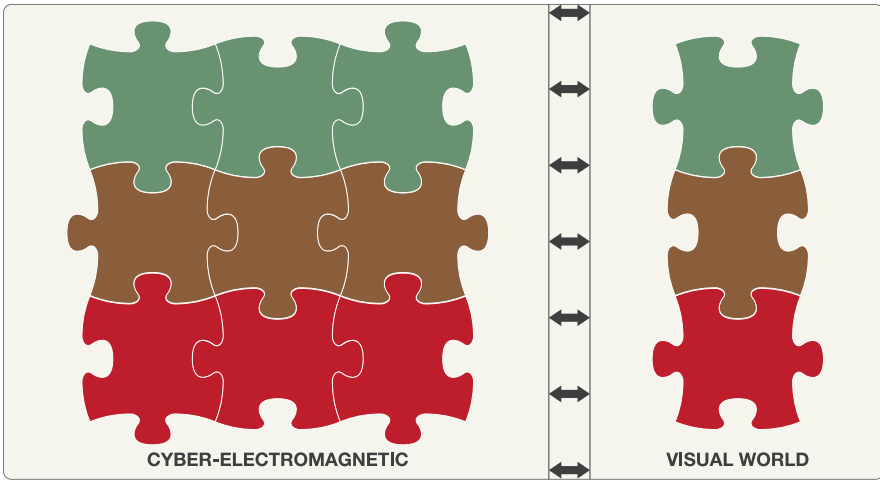


Figure 5.B.4: The Visual and Cyber-EM worlds

Figure 5.B.4 breaks the physical plane into the visual world and the cyber-electromagnetic world.

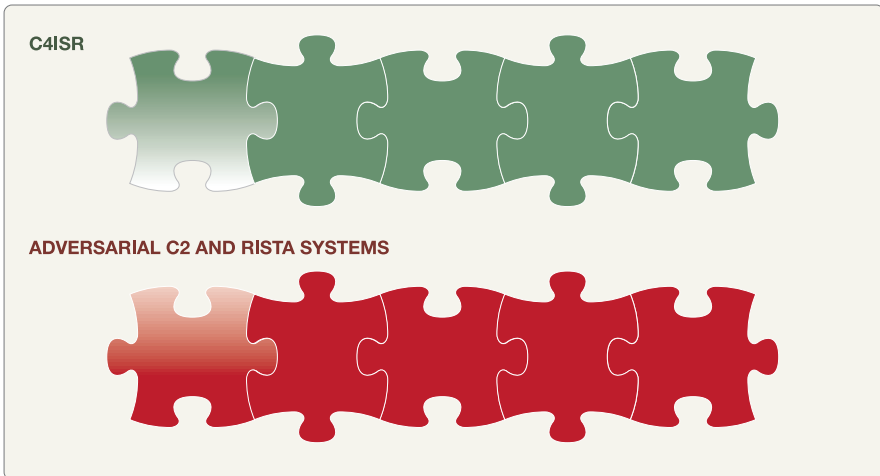


Figure 5.B.5: Friendly and Adversarial C4ISR Systems

Friendly and enemy C4ISR architectures fit into the land operating environment, as shown in Figure 5.B.5.

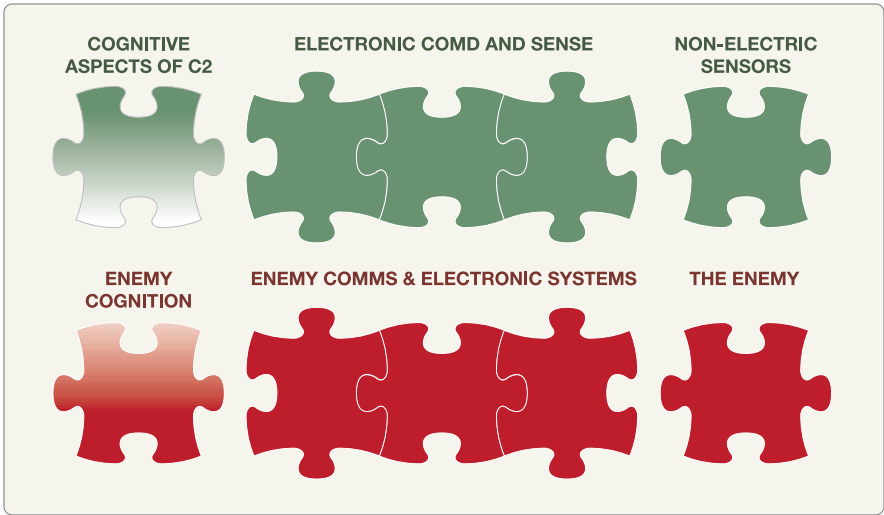


Figure 5.B.6: Breakdown of C4ISR

C4ISR includes aspects of the physical and psychological planes encompassing the visual and cyber-electromagnetic worlds. It is those three puzzle pieces in the middle of each of the friendly, neutral and adversarial puzzle strips that collectively describe the cyber-EM component of the land operating environment. The breakdown of the strips in Figure 5.B.5 is shown in Figure 5.B.6.

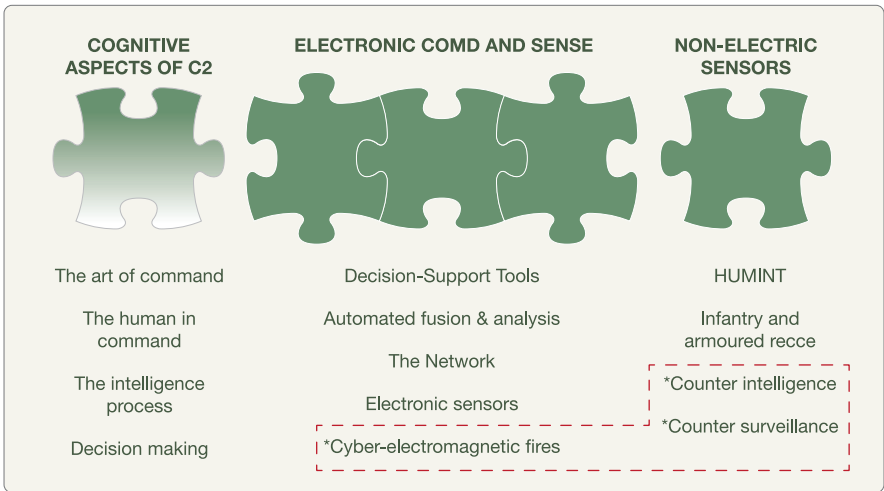



Figure 5.B.7: The Friendly C4ISR System

Figure 5.B.7 presents a detailed breakdown of friendly C4ISR architecture, listing several examples of the cognitive aspects of C2, the electronic aspects



of the Command and Sense operational functions, and non-electronic sensors within the ISR system. These examples are shown in green lettering directly below their appropriate C4ISR component. Depicted inside the red lines in Figure 5.B.7 are activities that are part of the cyber environment (such as cyber-electromagnetic fires) and the ISR system which are often included in discussions of friendly C4ISR but which actually fit better within the Act and Shield functions.

C4ISR is not a component of cyber, just as cyber is not a component of C4ISR—there is no C5ISR. The cyber environment is a component of the physical plane (hardware, software, electrons, and energy), whereas the C4ISR process includes aspects of both the physical and psychological planes. The physical cyber aspects of C4ISR include those that relate to Comd and Sense only. Extending the description of C4ISR to include other sub-components of cyber relating to Act and Shield would be counter-productive and would confusion.

CHAPTER 6

CONCLUSION



Source: Combat Camera

“Unmanned systems represent a potential future paradigm shift in the way land operations are conducted. The Army’s experimentation campaign plan must incorporate robotics to the greatest extent possible, providing a feedback mechanism necessary for honing the concepts presented here and further guiding build and acquisition efforts.”

—Major Jim Gash, *No Man’s Land: Tech Considerations for Canada’s Future Army*

The technological capabilities discussed in this compendium of future army concepts represent important considerations for the Army capability development process. Although they are critical capability areas for the future army, that does not imply the luxury of dealing with them down the road. Although space, cyber, and autonomous systems may not be of immediate concern, especially in a time of fiscal restraint, preparing ourselves now for the future makes a great deal of sense. The potential return on investment gained from capability development in these three areas represents tremendous value added to our relatively small force.

Unmanned systems represent a potential future paradigm shift in the way land operations are conducted. The Army's experimentation campaign plan must incorporate robotics to the greatest extent possible, providing a feedback mechanism necessary for honing the concepts presented here and further guiding build and acquisition efforts. Thinking about the incorporation of robotics now will ensure the timely fielding of appropriate systems with high degrees of acceptance by soldiers.

Similarly, understanding just how vulnerable space-based systems are, we must honestly assess of how land operations could be conducted without them. In order to benefit from the force enhancement capabilities traditionally associated with space-based systems, we must think of new ways to derive those capabilities from other sources. Seminar wargaming and simulation in synthetic environments represent potential ways ahead for exploring Army options.

Because so much of the Army's current investment is directly related to C4ISR, the Army must understand the cyber environment: what it is, its vulnerabilities, and the opportunities created by technological convergence. The C4ISR architecture must be protected as vital ground, as command and control of friendly forces is executed through it. In a similar fashion, as the cyber-electromagnetic environment is a shared space, the Army should make best use of any capability that could exploit a network-enabled adversary through the adversary's own reliance on the electronic aspect of their C4ISR systems. Exploiting advantages offered in cyber and space, and through the use of unmanned systems, ought to be a priority effort for the Army.

The capability development process must now move forward in maturing the concepts presented in this volume, finalizing concept development and experimentation (CD&E), and conducting further research where needed, especially in the more contentious areas. The Army will not be able to move



the yardstick forward by itself. CAF joint organizations in the force development community and the warfare centres resident in the other services should be engaged in order to ensure that these Army concepts fit well with the thinking of our CAF partners. The Army will not control space or cyber, and it will not be able to afford all the robotic systems that it might like to have, but it will rely on all three capability areas for success. Close collaboration with the capability development community of practice represents the best way ahead. 🇨🇦

AUTHOR

MAJOR JIM GASH, CD · FUTURE CONCEPTS TEAM

BIBLIOGRAPHY

Albus, James S. *Features of Intelligence Required by Unmanned Ground Vehicles*. National Institute of Standards and Technology, Gaithersburg, MD. 29 July 2010: http://www.isd.mel.nist.gov/documents/albus/Features_of_Intelligence.pdf.

Anderson, Kenneth. "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform." *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136.

Arkin, Ronald C., et al. *Responsibility and Lethality for Unmanned Systems: Ethical Pre-mission Responsibility Advisement*. Technical Report GIT-GVU-09-01, Georgia Institute of Technology. 29 July 2010: <http://www.cc.gatech.edu/~alanwags/pubs/GVU-TR-09-01.pdf>.

BAE Systems. *Unmanned Ground Vehicles Electronic Press Kit*. 29 July 2010: http://www.baesystems.com/ProductsServices/bae_prod_elec_press_kits_epks.html.

Barrett, Dr. Edward. "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform." *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136.

Board on Army Science and Technology. *Technology Development for Army Unmanned Ground Vehicles – Summary*. The National Academies, January 2003. *The National Academies Press*. 29 July 2010: http://www.nap.edu/catalog.php?record_id=10592.

Boot, Max. "The Paradox of Military Technology." *The New Atlantis*. (Fall 2006): 13-31. 29 July 2010: <http://www.thenewatlantis.com/publications/the-paradox-of-military-technology>.

Cowan, Thomas H. *Theoretical, legal and ethical impact of robots on warfare*. USAWC Strategy Research Project, US Army War College: Carlisle Barracks, PA. DTIC. 29 July 2010: <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA469591>.

Crispin, Ben. "What Killed the Robot Soldier?" *Strange Horizons*. 10 November 2008. 29 July 2010. <http://www.strangehorizons.com/2008/20081110/crispin-a.shtml>.

Department of Defense. *Office of the Secretary of Defense Unmanned Systems Roadmap 2007–2032*. 10 December 2007. Joint Robotics. 29 July 2010: [http://www.jointrobotics.com/documents/library/Office%20of%20the%20Secretary%20of%20Defense,%20Integrated%20Unmanned%20Systems%20Roadmap%20\(2007-2032\).pdf](http://www.jointrobotics.com/documents/library/Office%20of%20the%20Secretary%20of%20Defense,%20Integrated%20Unmanned%20Systems%20Roadmap%20(2007-2032).pdf).

Department of Defense. *Office of the Secretary of Defense Unmanned Systems Roadmap 2009–2034*. 29 July 2010: <http://www.acq.osd.mil/psa/docs/UMSIntegratedRoadmap2009.pdf>.

Department of the Army. *Robotics Strategy White Paper*. 19 March 2009. 29 July 2010. <http://www.futurefastforward.com/military-intelligence/1302-robotics-strategy-white-paper-27309>.

Deputy, Samuel N. *Counterinsurgency and Robots: Will the Means Undermine the Ends?* Paper submitted to the Faculty of the Naval War College, Newport RI, 04 May 2009. DTIC. 29 July 2010: <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA503005>.

Directorate of Combat Systems Engineering Management. *Explosive Ordnance Disposal Remotely Operated Vehicle: Updated Fielding Plan*. 19 January 2010. Project 00001111. J.T. Hewitt. "RE: Unmanned Vehicle Naming Convention." E-mail to Major J.C. Gash. 26 February 2010.

Donnithorne-Tait, Dewar. "Unmanned Systems: A Defence Perspective" *Frontline Defence* (Sept/Oct 2009): 19–24. 29 July 2010: http://www.alberta-canada.com/documents/AIS-AERO_UnmannedSystems-DefencePerspective.pdf.

Edwards, Sean J. A. *Swarming and the Future of Warfare*. Santa Monica, CA: RAND Corporation, 2005.

Fagan, Michael S. "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform." *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136.

Fehrenbach, T.R. *This Kind of War: The Classic Korean War History*. New York: Brassey's, 2001.

Fielding, Lieutenant Colonel Marcus. "Robotics in Future Land Warfare." *Australian Army Journal*. 3.2 (Winter 2006): 99–108. 29 July 2010: http://www.defence.gov.au/army/lwsc/docs/aa_j_winter_2006.pdf.

Finn, William. "Don't Believe the Bunny: Power and Unmanned Systems." *Amrel*. 2 March 2010. 29 July 2010: <http://www.commoncontrolnow.com/download/Dont-Believe-the-Bunny-Power-and-Unmanned-Systems-Discussion.pdf>.

Finn, William. "Radio Control and Unmanned Systems." *Amrel*. 16 February 2010. 29 July 2010: <http://www.commoncontrolnow.com/download/Radio-Control-and-Unmanned-Systems-Overview.pdf>.

Foss, Marek. *What are autonomous weapon systems and what ethical issues do they raise?* 30 March 2008. 29 July 2010: http://www.marekfoss.org/misc/Autonomous_Weapons.pdf.

Franke, Jerry L., et al. *Holistic Contingency Management for Autonomous Unmanned Systems*. Lockheed Martin. 29 July 2010: <http://www.atl.lmco.com/papers/1344.pdf>.

Gage, Douglas W. "UGV History 101: A Brief History of Unmanned Ground Vehicle Development Efforts." *Unmanned Systems Magazine*. 13.3 (Summer 1995): 1–9. 29 July 2010: <http://www.spawar.navy.mil/robots/pubs/ugvhist95-nopix.pdf>.

Gentry, John A. "Doomed to Fail: America's Blind Faith in Military Technology." *Parameters*. (Winter 2002-03): 88–03. 29 July 2010: <http://www.comw.org/rma/fulltext/0212gentry.pdf>.

Goldsmith, Major D.A. *Robots in the Battlespace: Moral and Ethical Considerations in the Use of Autonomous Mechanical Combatants*. Canadian Forces College JCSF 34. 29 July 2010: <http://www.CAFc.forces.gc.ca/papers/csc/csc34/exnh/goldsmith.pdf>.

Hanon, Leighton. *Robots on the Battlefield – Are We Ready for Them?* American Institute of Aeronautics and Astronautics, Inc. Chicago, IL. September 2004. 29 July 2010: http://pdf.aiaa.org/preview/CDReadyMUAV2004_1007/PV2004_6409.pdf.

Hew, Patrick Chisan. *The Generation of Situational Awareness within Autonomous Systems – A Near to Mid Term Study – Issues*. DSTO-GD-0467, Australian Government Department of Defence – Defence Science and Technology Organization. 29 July 2010: <http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/4560/1/DSTO-GD-0467.PR.pdf>.

Huang, Hui-Min, et al. *A Framework for Autonomy Levels for Unmanned Systems (ALFUS)*. Presented at AUVSI's Unmanned Systems North America 2005, Baltimore, MD. June 2005. 29 July 2010: http://www.nist.gov/customCAF/get_pdf.CAFm?pub_id=824538.

Huang, Hui-Min, et al. *Autonomy Levels for Unmanned Systems (ALFUS) Framework: An Update*. Presented at 2005 SPIE Defense and Security Symposium, Orlando, FL. 29 July 2010: http://www.nist.gov/customCAF/get_pdf.CAFm?pub_id=822672.

Institut für Religion und Freiden. *Interview with Armin Krishnan*. 23 November 2009. 29 July 2010: http://www.irf.ac.at/index.php?option=com_content&task=view&id=306&Itemid=1.

Jackson, John Edward. "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform." *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136.

Juberts, Maris and Barbera, Anthony. "Status report on next generation LADAR for driving unmanned ground vehicles." *NIST*. Proc of SPIE Vol. 5609: 1–2. 29 July 2010: http://www.isd.mel.nist.gov/documents/juberts/5609_2.pdf.

Krishnan, Armin. *Killer Robots: Legality and Ethicality of Autonomous Weapons*. Burlington, VT: Ashgate Publishing Company, 2009.

Kroske, Jens, et al. "Trusted Reasoning Engine for Autonomous Systems with an Interactive Demonstrator." *Codex*. Issue 5 (Winter 2009): 61–65. 29 July 2010: http://www.science.mod.uk/codex/issue5/journals/documents/codex5_journals_2.pdf.

Laird, Robert T. "Evolving U.S Department of Defense Unmanned Systems Research, Development, Test, Acquisition & Evaluation (RDTA&E)" *SPIE*. Proc. 7332: Unmanned Systems Technology XI, Defense Security Symposium. Orlando, FL, 13–17 April 2009. 29 July 2010: <http://www.spawar.navy.mil/robots/pubs/SPIE-7332-51.pdf>.

Land Operations 2021: Adaptive Dispersed Operations – The Force Employment Concept for Canada's Army of Tomorrow. Ed. Major Andrew B. Godefroy. Kingston, ON: Department of National Defence, 2007. 29 July 2010: http://www.army.forces.gc.ca/DLCD-DCSFT/specialPubs_e.asp.

Lefkow, Chris. *US Army Lt Gen Wants Unmanned Ground Vehicles*. Agence France-Presse. 12 August 2009. 29 July 2010: <http://www.defensenews.com/story.php?i=4231507>.

Makin, N.S. *Future Warfare or Future Folly? Autonomous Weapon Systems on the Future Battlefield: An Assessment of Ethical and Legal Implications in Their Potential Use*. Master of Defence Studies Research Project. Canadian Forces College JCSP 34. 25 April 2008. 12 April 2010 <http://www.CAFc.forces.gc.ca/papers/csc/csc34/mds/makin.doc>.

McDaniel, Erin A. *Robot Wars: Legal and ethical dilemmas of using unmanned robotic systems in 21st century warfare and beyond*. Thesis presented to Faculty of US Army Command and General Staff College, Fort Leavenworth, Kansas. 2008. 29 July 2010: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA502401&Location=U2&doc=GetTRDoc.pdf>.

Nardi, Major Gregory J. *Autonomy, Unmanned Ground Vehicles, and the US Army: Preparing for the Future by Examining the Past*. School of Advanced Military Studies, USACGSC, Fort Leavenworth, KS, AY 2008-09. 29 July 2010: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA506181&Location=U2&doc=GetTRDoc.pdf>.

Nguyen, Hoa G., et al. "Land, Sea, and Air Unmanned Systems Research and Development at SPAWAR Systems Center Pacific." *SPIE* Proc. 7332: Unmanned Systems Technology XI, Orlando, FL, April 14-17, 2009. 29 July 2010: <http://spiedl.aip.org/getpdf/servlet/GetPDFServlet?filetype=pdf&id=PSISDG00733200000173321I000001&dtype=cvips&prog=normal>.

RAND Corporation. *Balancing Rapid Acquisition of Unmanned Aerial Vehicles with Support Considerations*. Research Brief within parameters of Project Air Force. Santa Monica, CA. 2005. 29 July 2010: http://www.rand.org/pubs/research_briefs/2005/RAND_RB176.pdf

Sharkey, Noel. "Grounds for Discrimination: Autonomous Robot Weapons" *RUSI Defence Systems*. (October 2008): 86–89. 29 July 2010: <http://www.rusi.org/downloads/assets/23sharkey.pdf>.

Singer, P.W. "Robots at War: The New Battlefield." *Wilson Quarterly*. (Winter 2009) 29 July 2010 <http://www.wilsonquarterly.com/article.CAFm?aid=1313>.

Singer, P.W. "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform." *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136.

Singer, P.W. "Wired for War? Robots and Military Doctrine." *Joint Force Quarterly*. 52.1 (2009): 104–110. 29 July 2010. http://www.brookings.edu/articles/2009/winter_wired_singer.aspx.

Sparrow, Robert. "Killer Robots" *Journal of Applied Philosophy*. 24.1 (2007): 62–77. 29 July 2010: <http://www.sevenhorizons.org/docs/SparrowKillerRobots.pdf>.

Stocker, Harold. *Autonomous Intelligent Systems: Opportunities and Needs for the CAF/DND*. Defence Research and Development Canada. Technical Memorandum TM-2003-004, July 2003.

Stentz, Anthony, et al. *Real-Time, Multi-Perspective Perception for Unmanned Ground Vehicles*. Carnegie Mellon. 29 July 2010: <http://www.frc.ri.cmu.edu/~axs/doc/auvis03.pdf>.

Sullivan, Michael J. "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform." *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136.

Tierney, John F. "Statement given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform." *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136.

Trebes, Tanya L. "Agile Robotics." *Army* (March 2010): 99–104.

Trentini, M., D. Purdy, and S. Bogner. *Autonomous Land Systems applied to Indirect Fire Support 2005-2020: A Technology Assessment*. Defence Research and Development Canada. Technical Report TR 2003-134, November 2003.

Varcholik, Paul. *Interactions and Training with Unmanned Systems and the Nintendo Wiimote*. University of Central Florida. Paper No. 8255 presented at Interservice/Industry Training, Simulation, and Education conference 2008. 29 July 2010: <http://www.bespokesoftware.org/publications/IITSEC%202008.pdf>.

Weatherington, Dyke D. "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform." *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136.

Winslow, Lance. *Unmanned Vehicle Robotic Warfare: Hide and Seek Strategies*. Online Think Tank, 18 May 2007. 29 July 2010: <http://www.worldthinktank.net/pdfs/unmannedvehiclerobotic.pdf>.

Wolf, Kevin J. "Testimony given before the National Security and Foreign Affairs Subcommittee of the Committee on Oversight and Reform." *Rise of the Drones: Unmanned Systems and the Future of War*. 23 March 2010: http://www.oversight.house.gov/index.php?option=com_jcalpro&Itemid=19&extmode=view&extid=136.







NO MAN'S LAND: TECH CONSIDERATIONS FOR CANADA'S FUTURE ARMY

Looking into the future, one might identify several environments where humans may not easily pass, or in some cases dare not tread. Those contested areas, often referred to as “no man’s land,” exist not only in the human dimension of the future army but in the technological dimension as well. *No Man’s Land: Technological Considerations for Canada’s Future Army* tackles this complex subject head on and offers a detailed analysis of three key evolving areas in the field—unmanned systems, cyberspace and space-based capabilities—each of which will play a significant role in the success of all future land operations.

CANADIAN ARMY LAND WARFARE CENTRE

The Canadian Army Land Warfare Centre serves as the army’s intellectual foundation for the development of overarching concepts and capabilities for tomorrow and into the future. It is responsible for delivering concept-based, capability-driven tenets and specifications for force structure design; drawing up the army’s concept development and experimentation plan; serving as a focal point for connection with other warfare centres, government departments, partner nations, external agencies and academia; and delivering high-quality research and publications in support of the Canadian Army’s force development objectives.

