UNCLASSIFIED

AR-006-775

DSTO AUSTRALIA

ELECTRONICS RESEARCH LABORATORY

Information Technology Division

REPORT
ERL-0573-RE

TOWARDS A C^3I STRATEGIC PLAN PHASE 1 : PRELIMINARY CONSIDERATIONS

by

Victor C. Sobolewski

SUMMARY

The 1987 Defence White Paper highlights important developments, either put in place or foreshadowed, relating to the ADF's capabilities in Command, Control, Communications and Intelligence (C^3I). The more recent Defence Strategic Planning and Force Structure Review stress the key role of C^3I in underpinning the principal roles of Defence and of the ADF.

A Strategic Plan for C^3I is required to manage the development and acquisition of future and long-term ADF C^3I requirements in a consistent, coordinated and effective way. Such a Strategic Plan will need to : identify the objectives for C^3I as well as the resources required to achieve these; specify a C^3I goal architecture; and propose a road map or "Migration Plan" to transition from the ADF's existing or currently proposed C^3I systems to the envisioned state-of-the-art C^3I systems.

This Initial Report considers the basic problems associated with C^3I development; reviews technologies, tools and methods to support this; and makes recommendations which form the first phase of a C^3I Migration Plan.

FEB 92

COPY No. 5

APPROVED FOR PUBLIC RELEASE

POSTAL ADDRESS: Director, Electronics Research Laboratory, PO Box 1500, Salisbury, South Australia, 5108.

UNCLASSIFIED

CONTENTS

FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

1. The acquisition by the ADF of modern, computer-based Command, Control, Communications, and Intelligence (C^3I) capability has been given high priority in the 1987 Defence White Paper and in the latest Strategic Planning and Force Structure Reviews.

2. A **C^3I Strategic Plan** to manage the development and acquisition of ADF C^3I systems is required. This will need to describe a consistent and integrated approach to meeting the ADF's C^3I requirements; identify resources; specify a C^3I goal architecture; and develop a Migration Plan to transition from the ADF's existing C^3I systems to the envisioned evolving state-of-the-art systems. It is anticipated that the ADF will then develop a C^3I Master Plan and Migration Plans for specific ADF C^3I systems.

2. **This Report** considers the basic problems associated with C^3I development, proposes a C^3I development and acquisition strategy based on **"Evolutionary Acquisition"**, reviews technologies, tools and methods to support this, and makes a number of recommendations which go some way towards the first phases of a Migration Plan.

4. **C^3I**, at its highest level of abstraction, **is about the management of Defence resources based on information to achieve a given mission or objective.**

5. The **basic C^3I process** involves the sub-processes of : (1) **surveillance and information collection**; (2) **transforming this into "intelligence"** about an existing or potential enemy, his composition, location, state-of-readiness, and probable intent; (3) **assessing the resulting situation,** with reference to the status, location etc of own Defence assets, and **deciding on the best course of action**; (4) **communicating this course of action,** via orders, tasks and plans to own forces **for action and execution;** and (5) **monitoring the execution of actions.**

6. From this the basic operational C^3I system architecture follows, consisting of :

(1) A **"Surveillance and Information Collection System" (SICS),** consisting of a number of sensors and other surveillance and information collection assets, and personnel and procedures, which provide a commander the means to collect, in a timely fashion and in sufficient detail and accuracy, information on the current state, disposition and location of potential and existing threats, and of the surrounding environment (terrain, weather etc).

(2) An **"Intelligence and Own-Forces Information System" (IOFIS)**, consisting of computer-based facilities, staff and procedures, which provide the means to maintain, collate, evaluate, analyse, integrate, aggregate or fuse, and interpret information collected and obtained from the SICS, to create intelligence on the past, present, and likely state, disposition, location, and intent of existing or potential threats, and distribute this in a timely fashion, to the commander and other authorised users.

In addition, there needs to be a means to maintain, update and collate, the operational and administration information available on, or reported by, own forces on their state, readiness, state of supply, disposition and location.

(3) A **"Command Support System" (CSS),** consisting of primarily computer-based facilities, staff and procedures, which provide the commander and his staff the means to access intelligence and information in a suitable form and in a timely fashion, and which together with decision and planning aids and other utilities, including communications, support him in fulfilling his command and control role.

(4) A **"Communications System" (CS),** which provide communications between the C^3I (sub)systems, and distributes data, information, orders and tasking, and as required intelligence, to authorised C^3I system users.

(5) A fifth (sub)system, the **"Life-cycle Support System"**, necessary for the efficient and consistent development and management of the C^3I system, is also required (para 13 below).

Each of these proposed (sub)systems is described in some detail, together with their likely associated problems and issues.

7. **C^3I is beset with two intertwined major sets of difficulties.** One set of difficulties stems from a number of uncertainties and complexities which seem to be fundamental to **C^3I development.** The result is that **C^3I requirements and functionalities cannot be specified upfront, rather they evolve and become defined over time**. The other set of difficulties is associated with **C^3I acquisition,** and stems from the current defence system acquisition process which requires, upfront, a well defined and sensibly complete functional specification of the system to be procured; this, due to the first set of difficulties, is not possible.

8. The uncertainties and complexities which bedevil C^3I development, and which are described in some detail in the Report, include : confusion in, and incompleteness of, definitions in the C^3I field; uncertainty of C^3I system goals and missions; uncertainty as to the identity of C^3I system "stakeholders"; the inevitable, but difficult to predict, changes in the threat, and the consequent changes in national strategic priorities, force structure, including possibly command and control structure, which require changes to C^3I system capabilities; the software-intensive nature of C^3I systems, superimposed on the currently recognised **"software crisis"**; the adversarial nature of C^3I, with electronic/information warfare being practiced and the consequent requirements for a global C^3I security architecture; the ever-continuing developments, and the demands from C^3I end-users for their inclusion, of commercial information technology and telecommunications products, the two key technologies on which C^3I rests on; and the serious absence of a theoretical and intellectual base for addressing C^3I.

9. The above listed uncertainties and complexities explain why **the environment for the analysis, design, development and acquisition of C^3I is fragile, uncertain and even hostile**. The conventional development and acquisition process currently in practice which requires detailed and sensibly complete specifications up-front, prior to any full-scale development and acquisition, does not and cannot sensibly apply to C^3I systems.

10. **The strategy recommended for C^3I development and acquisition is that of Evolutionary Acquisition (EA),which is based on the .. "analyse-a-little.. fund-a-little.. build-a-little.. test-a-little.. field-a-little"**..principle. This matches optimally C^3I development where requirements and capabilities change with time for the reasons mentioned above; and it involves the funding, subject to successful tests and trials results, and the incorporation, of sensible increments of increased functionality into systems which are in existence, and already fielded.

11. **EA is now increasingly being adopted by, inter alia, the US, NATO and France,** as the way ahead for developing and acquiring C^3I systems, who recognise the hurdles (mainly cultural and vested interests) in moving away from the traditional development and acquisition process.

12.The **benefits of** adopting **EA** have been demonstrated, and **include** :

(a) A working C^3I system, with some core operational capability, is in the hands of the user at any point in time.

(b) The EA process encourages interaction between C^3I system stakeholders, in particular between end-users and developers, assuring C^3I system development is in accord with user-requirements.

(c) Exploitation of the latest commercial developments in Information Technology and Telecommunications is enabled, and encouraged, by EA.

(d) A phased and incremental approach to budgeting, important in times of increasingly uncertain defence budgets, is a characteristic of EA.

13. To fully realise the benefits of EA for C^3I, any proposed C^3I architecture must be sufficiently robust yet flexible enough to accommodate changes in, and growth of, C^3I system capability over an anticipated whole-life of 15-20 years. Additionally, the tools and methods chosen to implement C^3I, as well as the implementation, must be consistent with, and support, EA. To those ends :

(a) A fifth C^3I (sub)system, the C^3I **"Life-cycle Support System" (LCSS),** to be located within DSTO, is necessary to manage and implement C^3I system development and growth over its whole life-cycle, according to the particular sections of the C^3I Strategic Plan and Migration Plan which relate to itself. The required LCSS technical and developmental facilities, and staff and resources, are described.

(b) **The C^3I architecture** - that is the framework according to which the various processes which constitute C^3I will be structured - **will be based on principles of "layering".** Such "layered" architectures have been implemented successfully in telecommunications and information systems, the two technologies which underpin C^3I. Existing C^3I capability can be improved on by modifying the corresponding "layer", or new capability can be introduced by inserting additional layers, while retaining existing layers. Such "layering" concepts match EA well.

(c) It is recommended that C^3I system analysis, design, software and testing be based on **"object-oriented methods".** Such "methods" reflect the C^3I problem representation, rather than reflect computer operation representation, as is the case with more traditional methods. Also these "methods" are more amenable to **software reuse.**

(d) The widest possible use of **"Open Systems" standards** is recommended to preclude proprietary implementations and single-vendor products "lock-in". The trend towards "Open Systems" will permit the use of multi-vendor, heterogeneous computer products, and, where applicable and suitable, **Commercial-off-the-shelf (COTS)** applications and systems software.

(e) **For communications, the widest use of the civil sector communications infrastructure is recommended,** in accordance with Defence directives, in particular the use of the **"Integrated Services Digital Network" (ISDN)** and its follow-on, the **"Broadband-ISDN"**, which will permit multi-media (voice; data; narrative/text; graphics; video; imagery; etc) information distribution and transmission between C^3I (sub)systems, and between authorised users.

(f) To support the above approach, the **"lessons learned"** from the practices pertaining to, and implementation by, the US and NATO of their C^3I systems **will be studied and heeded.** In addition, the widest collaboration at the technical/development and user levels with Allies, through existing collaborative agreements, is recommended.

14. A number of **recommendations** (33 in all) **are made in Section 11** of the Report. These **are offered as the first part of a C^3I Migration Plan.** They propose the C^3I infrastructure considered necessary to implement a C^3I Strategic Plan; recommend C^3I architectures, tools, and techniques relevant to C^3I; and propose some near-term R&D activities.

THIS PAGE INTENTIONALLY LEFT BLANK

1 Background

The 1987 Defence White Paper **(DOA87)** highlights important developments put in place or foreshadowed relating to the ADF's capabilities in Command, Control, Communications and Intelligence (C^3I). These developments are two-pronged, namely:

(a) the restructuring of the ADF's command arrangements, in particular by the formation of Headquarters ADF (HQADF) with its ADF Command Centre (ADFCC), and the creation of a joint operational command system through the appointment of Maritime, Land, and Air commanders, each with their own supporting operational Headquarters. This restructuring has been accomplished;

(b) the proposed development of automated/computer-based Command Support Systems, and the introduction of new communications systems to support operations and administration. The former, in particular, has been accorded a high priority.

More recent Defence Strategic Planning **(ASP90)** stresses the key role of C^3I as the underpinning necessary for the (successful) performance of the nine principal roles of Defence and the ADF listed in (ASP90). Additionally, Air Defence, one of these nine principal roles, has been singled out as requiring ..."an efficient C^3 system, integrating surveillance and intelligence sources (both ADF and Civil)"...

A number of proposals and Plans have been recently prepared for the way ahead in fields including Communications, Surveillance, and Information Systems (both for Administration and Operations). These, however, concern themselves with elements of, or associated with, C^3I, and not with an integrated, complete C^3I system.

In the most recent Defence Force Structure Review **(FSR91)**, primacy is given, out of the nine key Defence roles identified in **(ASP90)**, to "Command, Control, and Communications","Intelligence Collection and Evaluation" and "(Maritime) Surveillance". The latter two provide "early warning", and hence are central to the ADF's level of operational readiness. **The three areas, integrated together, constitute C^3I.** In addition, **(FSR91)** also requires that ..."In (C^3I-related) communications, the civil infrastructure will be used increasingly to meet Defence needs"...

It is generally accepted that C^3I is both complex and beset with many uncertainties. Consequently there is a widespread perception that the introduction of modern technology into C^3I systems is not being managed in a coordinated and effective way. To rectify the perceived inadequacies in this complex process, a " **Strategic Plan**" for C^3I for the ADF is the logical solution. Such a C^3I Strategic Plan, to which all ADF C^3I "stakeholders" would contribute, would need, inter alia, to describe a consistent and integrated approach to meet the ADF's C^3I requirements; identify the resources to achieve this; develop a robust C^3I goal architecture; and propose a strategy to transition the existing or currently proposed ADF C^3I systems in planned phases to the envisioned, state-of-the-art C^3I systems. Further such a C^3I Strategic Plan could form the basis on which the ADF can develop - together with ADF C^3I stakeholders - a more specific "C^3I Master Plan", together with associated C^3I Migration Plans, each specific to a particular ADF C^3I system.

The main mission of Electronics Research Laboratory of DSTO is to support Defence and the ADF in the fields of C^3I and Tactical Electronic Warfare, in particular, by providing strategic advice, assistance in procurement and life-cycle s pport for new equipment and undertaking appropriate research and development.

This report is an initial ERL contribution towards such a C^3I Strategic Plan. It considers the basic problems associated with C^3I and its development, proposes a C^3I development strategy, reviews technologies, tools and methods to support this, and makes recommendations which could form the first steps of an associated C^3I Migration Plan. It is preliminary only, as no formal discussions or interaction of any depth with HQADF or individual Services have been held.

2 Definitions

2.1 Current Definitions

A major problem bedevilling C^3I is the confusion in terminology, and incompleteness of definitions, pertaining to C^2 (Command and Control), C^3 (C^2 with "Communications"), and C^3I (C^3 with "Intelligence"). As recently as 1989, at a C^3 Technology conference sponsored by the US Defence Communications Agency **(DCA89)**, the first of the (five) major conference findings, was (the existence of) "Confusion between C^2 and C^3 Terminology", in particular as C^2 is a military and behavioural function, while C^3 intertwines technology with military behaviour. Concatenating another function such as "Intelligence" with C^3 further confuses and obscures the different disciplines and roles associated with each of these. To complete this confusion, acronyms such as "C^4I" (C^3I with "Computers") and even "C^4I^2" (C^4I with "Information") are occasionally come across. It is therefore necessary to distinguish each of these terms, so that what is meant by C^3I and associated terms and acronyms is clarified at the outset.

The following definitions have been extracted primarily from the Joint Services Staff Manual "Glossary", (JSP(AS)101, Edition 3, February 1984)**(JSP84).** Most definitions therein are based on the US Joint Chiefs of Staff **(USJCS88)** and NATO definitions. **However C^3I, as well as many C^3I-related terms, are undefined.**

Command and Control : The exercise of authority and direction by a properly designated Commander over assigned forces in the accomplishment of the mission. Command and Control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a Commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. **(USJCS88).**

Communications : A method or means of conveying information of any kind from one person or place to another.

Communication System : A system or facility capable of providing information transfer between persons and equipment.

Intelligence : The product resulting from the collection, evaluation, analysis, integration and interpretation of all information concerning one or more aspects of foreign countries or areas, which is immediately or potentially significant to the development and execution of plans, policies, and operations.

Information (Intelligence) : Unevaluated material of every description, including that derived from observations, reports, rumours, imagery, and other sources that, when processed, may produce intelligence.

Information : The meaning that a human assigns to data by means of the known conventions used in their representations. **(USJCS88).**

Data : Representation of facts, concepts, or instructions in a formalised manner suitable for communication, interpretation, or processing by humans or by automatic means. **(USJCS88).**

Information System : The organised collection, processing, transmission and dissemination of information in accordance with defined procedures, whether automated or manual. **(USJCS88)**

Surveillance : The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.

System : Any organised assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. **(USJCS88).**

There are no officially accepted or proposed definitions of C^3I or of a C^3I system. Several US DOD and NATO terms come close. These include :

(a) **Command, Control and Communications** (C^3) : The process and the means of accomplishing Command and Control. **(USJ88)**.

This definition has been augmented by, and coupled with, the following **(DCA86)**:

C^3 Capabilities will include resources to:

* Obtain, report, communicate, process, analyse, synthesize, display, and disseminate information to support Command Planning and Decision Making.
* Formulate alternative Courses of Action.
* Make Decisions.

To be consistent with the previous definitions, in particular with the usage of "information" in the first"bullet", the following is proposed (in lieu of the first "bullet"):

" * Obtain, report, communicate, process, analyse, and synthesize information, and display and disseminate the resultant intelligence to support Command Planning and Decision Making."

(b) **Command, Control and Information System** : An integrated system of doctrine, procedures, organizational structure, personnel, equipment, facilities and communications which provides authorities at all levels with timely and adequate data to plan, direct and control their activities.

This is a NATO definition which has been accepted in JSP(AS)101; however it contains inconsistencies in the usage of "information" and "data", and omits "intelligence" altogether.

(c) **Command Support System** : An integrated information storage and retrieval system, together with the necessary personnel and utilities required to support a commander at any level.

This is from "JSP(AS)8 : Command and Control of ADF Operations", **(JSP(AS)8)** and comes pretty close to what a commander may expect a C^3I system to provide him.

2.2 Proposed C^3I Definitions

The following are offered as definitions of C^3I and C^3I System, and will be so used in this Report :

Command, Control, Communications and Intelligence (C^3I): The process and the means to accomplish Command and Control. The C^3I capabilities will include resources to:

(1) sense, collect, and obtain information;
(2) report and communicate information and data;
(3) process, analyse, collate, and synthesize appropriate information into intelligence;
(4) disseminate information and intelligence in a suitable format, and in a timely manner, to support Command Planning and Decision Making;
(5) formulate alternative Courses of Action;
(6) make Decisions;
(7) pass or communicate Decisions and any other orders and tasking to appropriate subsystems;
and (8) monitor events and course of action related to decisions, orders, tasking etc.

C^3I System : An integrated system of doctrine, procedures, organizational structure, personnel, equipment, facilities and communications which effect C^3I.

3 C^3I : Process and System Considerations

The above proposed definition for C^3I sensibly includes within itself the C^3I process. From this, a C^3I paradigm, the C^3I process and a C^3I systems-oriented view, identifying the major C^3I subsystems, follow in a straight-forward manner.

3.1 C^3I Paradigm

A **paradigm** is a set of concepts or a model which represent a process; its role is to gain insight into the subject process, as well as to use it as the basis for developing specific instances of the process. When a given paradigm gains acceptance by a majority, it may become a "reference model", such as, for example, the ISO OSI 7-layer model representing the data communications process between computers.

A C^3I paradigm is a pattern which is general enough to be representative of the C^3I process for different echelons, different services, and different goals and missions. There is, as yet, **no C^3I reference model. (MAY88)** lists at least 16 different C^3I paradigms that have been used (and that after self-admitted non-exhaustive research!)
The C^3I paradigm that is developed herein is essentially based on the C^3 paradigm given in **(RUB88).**

Broadly,

> **C^3I is about the making of decisions on the use of (Defence) resources to carry out actions to achieve a given objective. The decisions are based on information obtained through observation and reporting.**

At the highest level of abstraction,

> **C^3I is about management of resources, based on information, to achieve a given objective.**

The "glue" binding state-of-the-art C^3I is Information and Communications Technology products, in particular, computers and telecommunications.

C^3I is effected in, and interacts with, an **environment**, the "region of interest", which is populated by the defence resources under control of a subject C^3I system ("own forces" and their assets), allied forces, friendly countries and their forces, neutral countries, potentially hostile countries, and existing hostile countries, and their respective forces. The "environment" includes the airspace, the surface, and (sea) sub-surface, their nature (topography, vegetation cover, seastate etc), weather and so on, in the region of interest, within which own forces, those of its allies, and of the enemy and his allies will, either in peacetime or during hostilities or war, carry out **"operations"** (see definition of "operation" below).

Figure 1 is a useful, yet simple, C^3I paradigm, based on one given in **(RUB88).** C^3I is essentially a continuous cycle of **observation** on the **environment**, which produces **information,** in the form of **reports,** based on which **decisions** are made (to meet some given objective), resulting in **orders** and **tasking** to carry out some **action** on the environment. The cycle begins anew by observation on the outcome of the action.

The above brief description of C^3I is generic and is applicable in both peacetime and during hostilities; to high-level, national C^3I as well as to lower echelon, tactical C^3I; and to the various single Services.
During peacetime, the C^3I process, through reporting from own forces, and through surveillance, observation, and collection of information by national assets and from allies, produces information which is massaged, processed, aggregated, fused etc, to produce "intelligence". This is then assessed and forms the basis on which decisions are made to structure, equip, base and deploy own forces to achieve the given peacetime Defence objectives ("deterrence", "operational readiness", "peacekeeping" etc). This particular instance of the C^3I process is achieved primarily through what we will call the "C^3I Administrative Loop" (or **"Cooperative C^3I Loop"**) (see Figure 2), and concerns itself with the management of own personnel and logistics, through cooperative reporting and observation (see the definition of "Administration" in the military/defence context below).

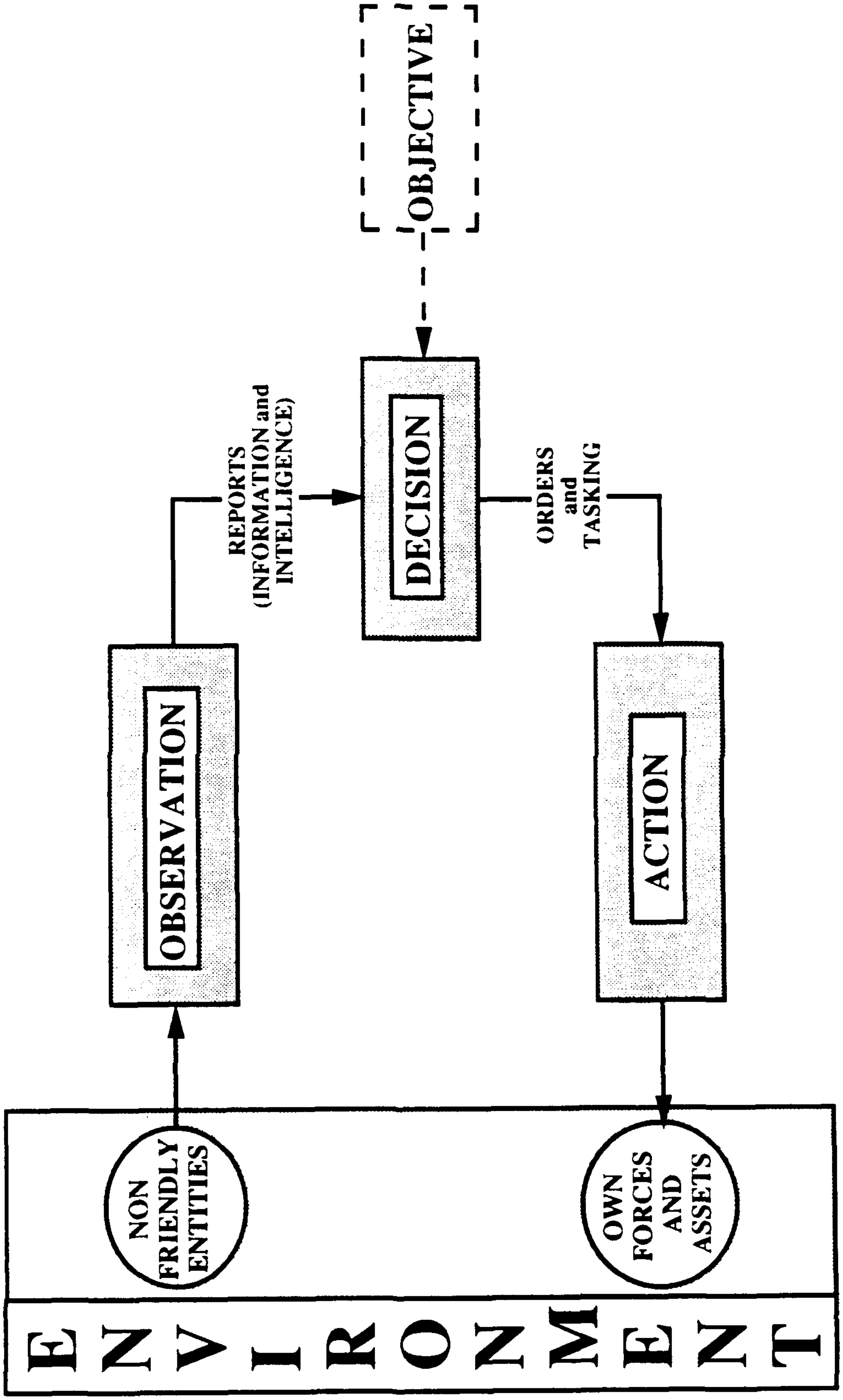


Figure 1 C^{3}I Process Paradigm (modified from RUB88)

During military emergencies, low-level conflict, or war, the missions and objectives of C^3I will change. Much of the C^3I decision making will be based on information gathered and processed into intelligence, from surveillance of, and observation and reporting on, non-cooperative/hostile entities. The missions and objectives of this particular instance of C^3I will be more immediate, and the surveillance- , information collecting/processing/transforming into intelligence- , assessment- , decision making-, and planning- activities, and the issuing of orders and tasking and effecting responses need to be more immediate as well as timely. That additional part of the C^3I process dealing with information collecting and intelligence on non-friendly/hostile entities is achieved through what we will call the "C^3I Strategic/Tactical Loop" (or **"Non-cooperative C^3I Loop"**); the latter term will be used.

The point that is being made by distinguishing, and identifying, the two "C^3I loops", is that C^3I deals with the management of own forces based on information obtained through two distinct information collection sub-processes:

(1) a **cooperative** information collection process effected through the reporting by, and on, own (and allied) forces, their status, position, wellbeing etc primarily via communications (and through a number of distinct reporting facilities dealing with personnel, logistics,and so on);

(2) a **non-cooperative** information collection process of surveillance, and collection of information including reporting by own troops, on **uncooperative** non-friendly/hostile elements, which is further processed into "intelligence", giving the enemy strength, position, status, and probable intent.

It is necessary at this stage to define several additional military terms (from **(JSP84)**):

Operation : A military action or the carrying out of a strategic, tactical, Service, training, or **administrative military mission**; the process of carrying on combat including movement, supply, attack, defence, manoeuvres needed to gain the objectives of any battle or campaign (own emphasis added).

Administration : The management and execution of all military matters not included in tactics and strategy; **primarily** in the fields of **logistics** and **personnel management** (own emphasis added).

Logistics : The science of planning and carrying out the movement and maintenance of forces.

3.2 C^3I Process

Following from the above and, in particular, from the definition of C^3I, the C^3I process can now be described by the following sequence of sub-processes :

(1) **collection of information,** via surveillance, reporting from own forces, and any other means, from the environment/area of operations, on the enemy, his allies and the physical environment in which they are located (via the "Non-cooperative C^3I Loop"); as well as on the status, readiness, location, well-being etc of own (and allied) troops (via the "Administration Loop" or "Cooperative C^3I Loop"):

(2) **transformation of (part of) that information (that on the enemy, terrain etc) into intelligence** by evaluation, analysis, fusion, and interpretation, to determine the enemy's strength, location, and probable intent;

(3) **assessment of the situation; generation of possible courses of action;** and **selection of a preferred course of action;**

(4) **planning a response** based on the selected course of action;

(5) **issue of orders and tasking** to all assets under command and control including to own troops, to surveillance sensors and assets, and to any other information collection and intelligence generation assets;

(6) **execution of response;**

(7) **monitoring of execution** of the response.

The cycle is restarted by reporting from own troops and surveillance reports and assessing the results of the immediate previous response.

Implicit in the above is :

(a) the availability of an **effective communications system** to support reporting from own troops (and allies); to support information collection and surveillance tasking; information transmission; transmission and distribution of intelligence to authorised recipients; to provide a secure command communications net to own forces; and for logistics and administrative support to effect and execute the response;

and (b) **a set of doctrines, procedures and an organization structure** which generally vary from national force to national force, and which, in the whole with C^3I, determines the success of operations.

Figure 2 illustrates the C^3I process.

The above described **C^3I process is generic** and is as old as warfare itself.

Centuries ago, the eye was the means of surveillance and collection of information in the area of operations, which, in the main, was the battlefield within sight of the commander (chief, king etc). The "transformation of information" into "intelligence", "situation assessment", "selection of courses of action", "planning responses", were all cerebral processes, carried out by the commander/chief/king etc, or, in some cases, with the help of his trusted advisers ("staff"). Orders were communicated and responses initiated by shouts, trumpets, flags etc, when and if these could be heard, or seen, in the tumult of battle ("communications"). "Organisational structure" was based on family and vassalage; "doctrine", invariably on physically destroying the opposing force.

In more recent times, technology has been the main driver for the changes to C^3I implementation. Forces now are widely dispersed in the area of operations, due to the nature of weapons and the changed nature of war and, in particular, due to speed and mobility. Surveillance and communications must cope with vast distances. Surveillance, for example, is now carried on from satellites; from ground-based "over-the-horizon" radars capable of detecting moving targets at distances of 2-3000 kms; by large sub-surface towed and fixed acoustic arrays; as well as by the more traditional means of obtaining information. Increasingly more and more information is being collected in shorter and shorter times. Forces can deploy over vast distances in shorter and shorter times (cf. the deployment of forces in the recent Persian Gulf conflict). Weapons have increasing ranges and shorter delivery times. To cope with all these developments, increasing use must be made of automated, computer-based means to process information, keep track of resources, and, wherever possible, support the commander and his staff in the exercise of his command and control functions, by keeping the **decision cycle** as short as possible and, in particular, shorter than the opponent's (ie **operating inside an opponent's decision cycle**). In addition, national and military command structures have changed, being now more distributed and, very likely, more complex. Finally, "traditional" roles for the military have been augmented by additional ones, such as, inter alia, overseas peacekeeping and participation in multi-national operations to meet international obligations; restoring services and other emergency functions after natural calamities; as well as other roles as may be determined by the Government of the day.

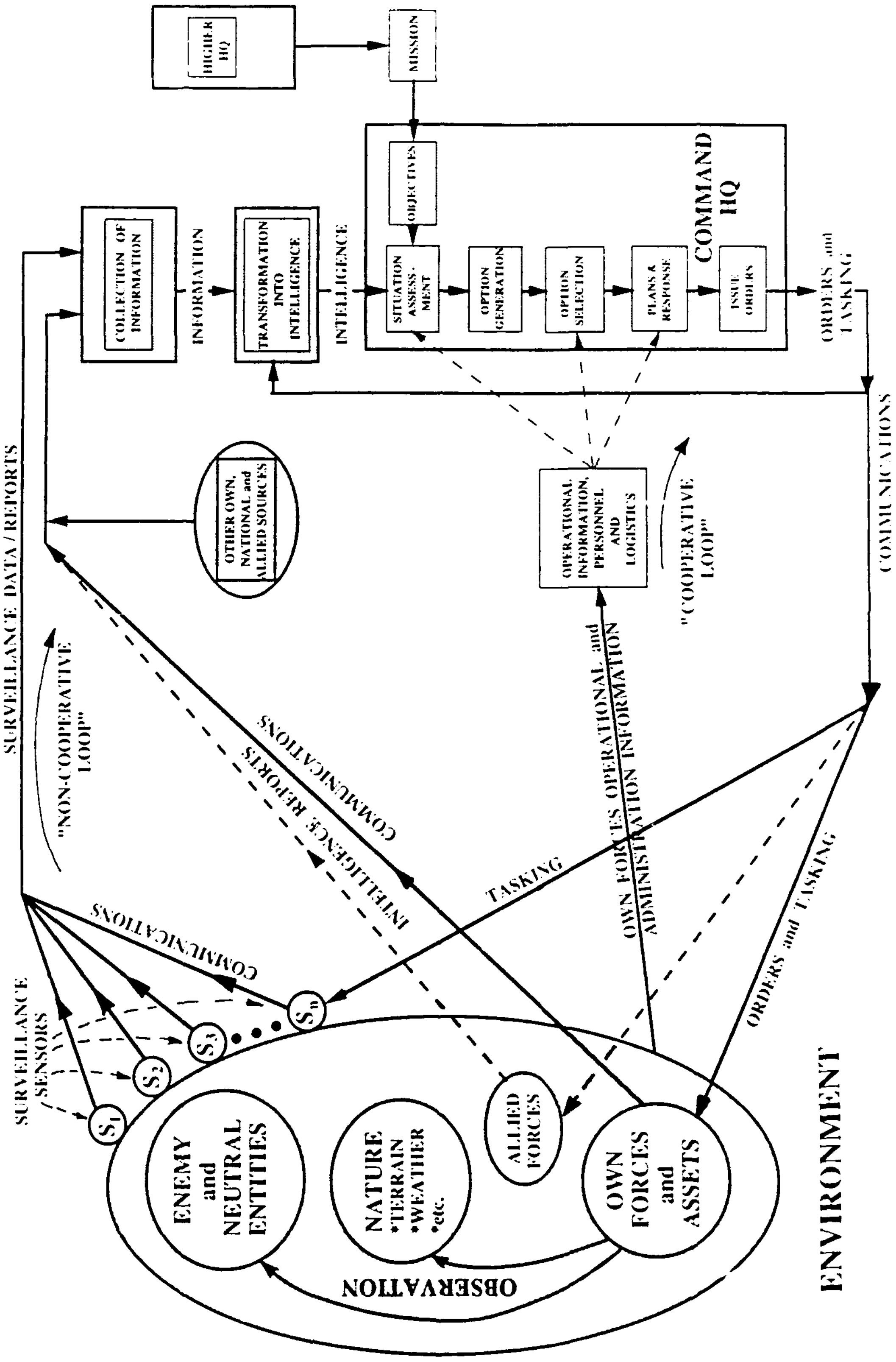


Figure 2 The C^{3}I Process

3.3 C^{3}I System

3.3.1 Existing ADF C^{3}I Systems

A "C^{3}I system" currently exists in the ADF and its constituent Services and has existed in Australia's military forces since her founding in 1788. At any point in time, this system reflected the current Government (or Colonial) defence policy, the command structure of the time, and the then-existing technology.

As indicated in Section 1, the following significant changes have occurred recently:

(a) New strategic assessments resulting in new Defence priorities;

(b) Significant changes to the command structure at the higher levels of the ADF;

(c) A number of developments in technologies pertinent to C^{3}I.

Partly as a response to this, a number of ADF C^{3}I projects are in place, some conceived since (DOA87), others having their beginnings before this. Some examples are :

(1) JP 2030 (HQADF Command Support System).

(2) Developments in Maritime HQ based on the OBU (OSIS Baseline Upgrade).

(3) AUSTACCS.

These and their capabilities, together with other related ADF projects, are briefly described in Sections 7.2.2.4 and 7.3.1.5. Each of these C^{3}I systems has some of the features of the C^{3}I process described above.

3.3.2 Generic C^{3}I System

The C^{3}I system and its component subsystems can now be described; this follows directly from Figure 2, which describes the C^{3}I process.

A C^{3}I system must have at least the following four (sub)systems:

(1) **Surveillance and Information Collection System (SICS)** : This is the means to collect in a timely fashion and in sufficient detail and accuracy, information on the current state, disposition and location of potential and existing threats and of the surrounding environment (terrain, weather etc) which forms the "region of interest" or, during conflict, the area of operations.

The SICS will consist primarily of a number of surveillance assets and sensors organic to assets under the command or control of a commander, or may be assigned to him by a higher HQ for the duration of the commander's mission. This will form the **Surveillance Subsystem.**

Of equal importance and additonally are the observation and reporting capabilities of own forces via organic communications networks. This will be called the **Information Collection Subsystem.**

The SICS needs access also to information from more traditional sources (eg Humint etc), as well as from Allied sources.

(2) **Intelligence and Own-Forces Information System (IOFIS)** : This is the means to store, maintain, collate, evaluate, analyse, integrate (or "fuse") and interpret information collected and obtained from the SICS, to create intelligence on the past, current and likely state, disposition, location, and intent of existing or potential threats, and distribute this in a timely manner, in a selection of standard, easily understood and assimilatable formats to the commander, his staff, and other authorised users.

In addition, there needs to be a means to maintain, update and collate, and integrate with the above intelligence picture as required, the information available, or reported from own (and allied) forces, on the the state, readiness, state of supply, disposition and location of own forces and assets and those of allies or other friendly troops.

The means and assets to generate **intelligence** on enemies or potential enemies ie on essentially **non-cooperative** entities, will be called the **Intelligence Subsystem (INTS).** It is associated with the "Non-cooperative C^{3}I Loop".

The means and assets to maintain, collate and update **information** on own, allied and friendly forces, ie on essentially **cooperative** entities, will be called the **Own-Forces Information Subsystem (OF-INFS).** It is associated with the "Cooperative C^{3}I Loop".

The two subsytems, although different, are associated together to form the IOFIS. It must be recognised that they will remain differently structured and staffed (sub)systems; and although both massage, manage, process, collate and store information, they use different sources of information (associated with the two different "Noncooperative" and "Cooperative" C^{3}I "Loops") and produce different products : intelligence about the enemy, and information about own forces and current assets. Together these products are used to create a "current situation assessment" on which decisions and plans are made.

(3) **Command Support System (CSS)** : The means which provide the commander and his staff access to intelligence and information in a suitable form and in a timely fashion, together with decision and planning aids and other utilities, including communications, to support him in fulfilling his command and control role.

This is sensibly the definition of a CSS in section 2.1(c), somewhat expanded to include decision and planning aids.

(4) **Communications System (CS)** : The means to provide communication between, and to distribute information and, as required, intelligence between the C^{3}I (sub)systems to, authorised users; between command echelons; and between lateral commanders and lateral C^{3}I systems.

The CS clearly needs to provide much more than the traditional voice and, more recently, data communications associated with the Command Net (the communications network which connects an echelon of command with some or all of its subordinate echelons for the purposes of command and control **(JSP84)**) and other reporting communications nets, such as for personnel management, logistics, and specific battlefield functional communications nets. Information and Intelligence pertaining to C^{3}I is increasingly becoming "multi-media" (ie a mix of data, formatted text, graphics, imagery, and even video), the distribution of which will require increasingly higher bandwidth digital communications networks between the geographically dispersed fixed and mobile C^{3}I system nodes.

The above C^{3}I (sub)systems are described more fully in Section 7.

A fifth C^{3}I (sub)system, the **(C^{3}I) Life Cycle Support System (LCSS)** is also deemed necessary. Its functions and justification, primarily on the basis of "evolutionary development and acquisition" which is required for C^{3}I systems, are described below in Section 5.5.

3.3.3 Procedures and C^{3}I Systems

A "**system**" by definition (section 2.1 above) consists of .."**an organised assembly of resources and procedures**".. Consequently associated with each of the above C^{3}I (sub)systems there will be groups of human resources organised to perform specific tasks according to procedures, some of which have been adopted by convention or convenience, while others are more formalised as **standing (or standard) operating procedures (SOP).**

> **Standard/Standing Operating Procedure (SOP)** : A set of instructions covering those features of operations which lend themselves to a definite or standardised procedure without loss of effectiveness. **(JSP84)**

The particular organisation of human resources associated with each C^{3}I (sub)system, and the procedures and SOPs laid down and used, have evolved over time from example, war-gaming, exercises, and cases of success in actual conflict. In the main, they still tend to reflect obsolescent organisations which are heavily man-dependent and C^{3}I systems which are message-oriented. Such procedures may include, say in the SICS, the procedures for tasking sensors for general surveillance, or for a specific target search; in the CSS, the organisation of the Commander's staff in their specific roles and duties; and so on.

Implicit in the definition of a "system" is that its components of "assemblies of resources and procedures" are "un:ted" and "organised", because they need to match and complement each other in the accomplishment of their specific (C^{3}I) system functions.

The recent evolution of C^{3}I systems towards computer-based technologies and systems is resulting in a new set of system resources which no longer necessarily match or complement the human resources and the procedures/SOPs in place in the C^{3}I systems they are improving on.

It is hypothesised that a key source of the difficulties and complexities of developing and implementing modern C^{3}I systems is, to a large extent, the mismatch resulting from trying to map what have been to date, human-oriented and personnel-intensive C^{3}I systems, with their associated human-organisation and procedures/SOPs, onto computer-based C^{3}I systems, which require different and, in many cases, simplified pro:edures/SOPs.This is essentially a problem of "reverse-engineering". It is treated in more detail in Section 4.2.

Figure 3 shows the proposed generic C^{3}I system with the interactions between the five (sub)systems, and in particular it shows that the control of the sensors and of the Intelligence and Information (sub)system is with the Commander, via tasking. It also shows the two information collection and processing loops, the "Cooperative" and "Non-cooperative" C^{3}I loops.

Figure 3 is generic and is not meant to represent any specific C^{3}I system. For such specific cases, the relative size and complexity of each (sub)system, the number of "cooperative C^{3}I loops" (ie the "personnel", "logistics", "reconnaissance", "fire control" etc reporting and tasking loops) will differ. The point where such loops begin, which is generally where its corresponding tasking orders originate, will also differ; for example, in Figure 2, which decomposes the CSS into functions, tasking for surveillance and intelligence requirements may originate after "situation assessment", while "logistics" status updates may be required at the 3 points in the process, as indicated on that Figure.

Specific C^{3}I system configuration and implementation will depend on C^{3}I system "missions and goals", and their related requirements and functionalities, and after the uncertainties and complexities associated with each such C^{3}I system have been resolved. This is discussed in the following Section.

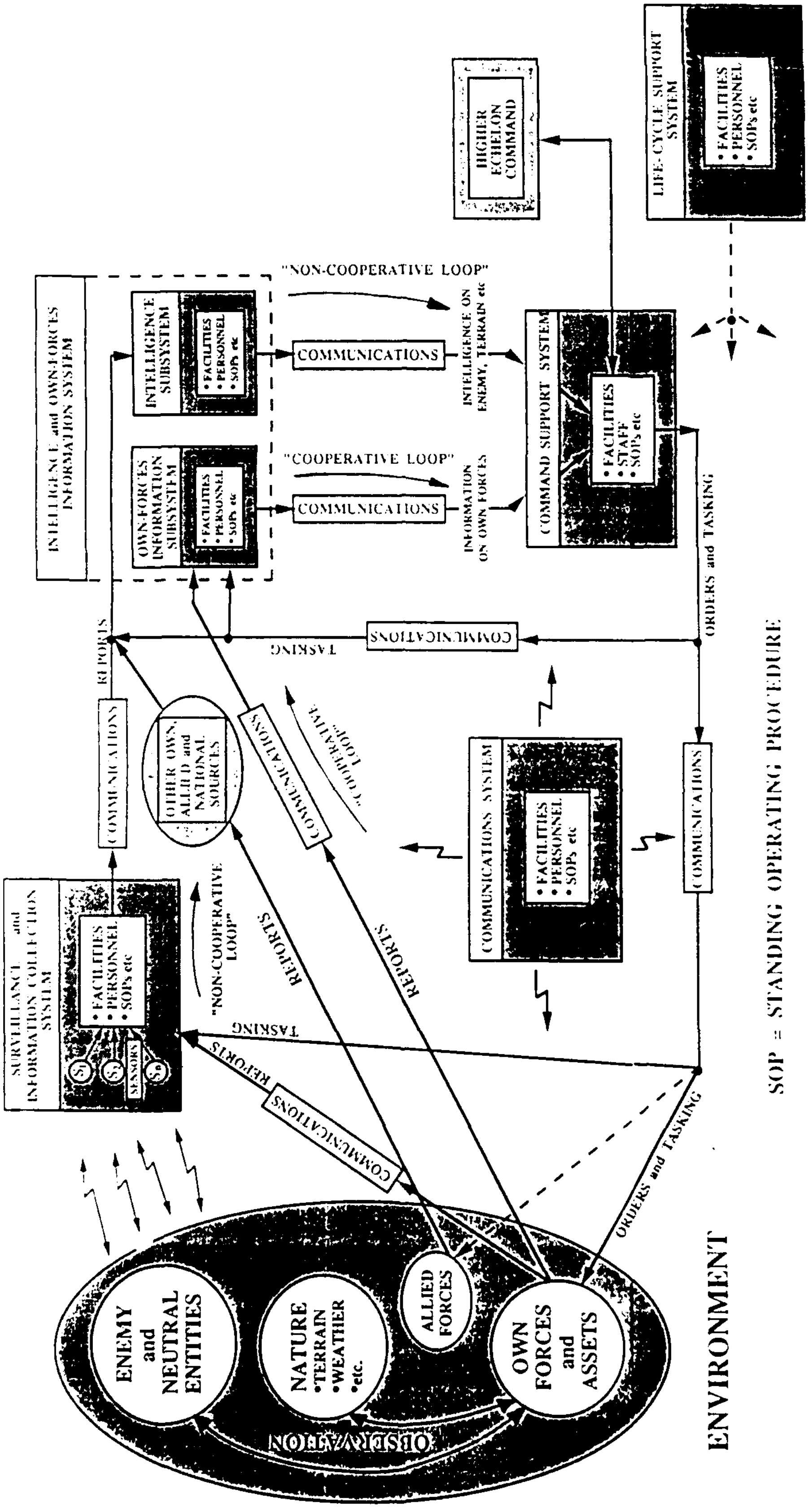

ENVIRONMENT
ENEMY and NEUTRAL ENTITIES
NATURE •TERRAIN •WEATHER •etc.
ALLIED FORCES
OWN FORCES and ASSETS
OBSERVATION
SURVEILLANCE and INFORMATION COLLECTION SYSTEM
• FACILITIES • PERSONNEL • SOPs etc
SENSORS
COMMUNICATIONS
REPORTS
TASKING
"NON-COOPERATIVE LOOP"
OTHER OWN, ALLIED and NATIONAL SOURCES
"COOPERATIVE LOOP"
INTELLIGENCE and OWN-FORCES INFORMATION SYSTEM
OWN-FORCES INFORMATION SUBSYSTEM
INTELLIGENCE SUBSYSTEM
INFORMATION ON OWN FORCES
INTELLIGENCE ON ENEMY, TERRAIN etc
COMMAND SUPPORT SYSTEM
• FACILITIES • STAFF • SOPs etc
HIGHER ECHELON COMMAND
LIFE-CYCLE SUPPORT SYSTEM
COMMUNICATIONS SYSTEM
ORDERS and TASKING
SOP = STANDING OPERATING PROCEDURE

Figure 3 Generic C³I System

4 Uncertainty and Complexity in C^3I

C^3I is bedevilled by **uncertainty** and **complexity**.

4.1 Organic C^3I Uncertainty

Uncertainty and its reduction is at the core of C^3I. A major role of any C^3I system is to remove as much as possible of the uncertainty that exists during conflict at any point in time, in particular by that part of the (C^3I) system which performs surveillance and the collection of information, and processing and fusing it into intelligence, generally under conditions of incomplete, ambiguous, often contradictory, and increasingly deliberately false, information.

However the uncertainty that is of concern here is of a more fundamental kind, and will be called "**organic C^3I uncertainty** ", because it is inherent in C^3I. Although it is primarily keenly felt at the initial stages of C^3I system development, this type of uncertainty is present throughout the life-cycle of any C^3I system.

The prime causes for "organic C^3I uncertainty" are :

(1) non-robust, ambiguous and incomplete C^3I definitions and terms;

(2) lack of clear C^3I system Missions and Goals statements;

(3) lack of identification of, and consultation with, all C^3I "stakeholders";

(4) changes to external factors over the C^3I system's life-cycle.

4.1.1 Uncertainty of C^3I Terms and Definitions

The meaning of C^3I terms is still in dispute, despite the term "command and control" and its derivatives having gained currency in the early Sixties. This in itself would not be of much importance, had it not led to counter-productive confusion between the roles of the end-users (namely a commander exercising command and his staff implementing control (together the "C&C function")), and those of the providers of a C^3I system, specifically of the Command Support System (which provides the technology integrated into a commander's existing system to help him carry out his C&C function). A C^3I system does not replace a commander!

A 1978 US DoD Defence Science Board study of C&C (**DSB78**) concluded then :

> ".. there is **almost no commonly understood vocabulary** (emphasis added) or conceptual framework for analyzing, designing, or evaluating Command and Control systems..."

Some 10 years later a similar complaint was voiced at a C^3 Technology conference sponsored by the US DoD DCA (**DCA89**) (previously referred in Section 2.1).

More recently, the presence of this definitional problem has been stated to be a prime reason for at least sixteen paradigms or models of the C^3I process currently existing, each differing from each other to a greater or lesser degree (**MAY88**). The lack of a standard or widely accepted C^3I paradigm ("C^3I reference model") has, in turn, diluted R&D efforts in this area.

As mentioned earlier, the term/acronym C^3I, despite its ever increasing usage, has yet to be officially defined. One likely reason for this may be that to date there has been - and still remains - a very strongly held view by the Intelligence community, that "I" is not organic to C^3I systems and that consequently C^3I should more properly be "C^3"; clearly such a view has significant consequences for any proposed architecture of C^3I systems.

Section 2, discussing and leading to the formulation of some new C^{3}I terms, was included at the outset to clear some of this confusion and uncertainty.

The usage of C^{3}I is retained in this report.

4.1.2 Uncertainty in C^{3}I Goals and Missions

Another set of difficulties, critical to the success if any proposed C^{3}I system, arises due to the uncertainty frequently associated with the mission (or goals, objectives, purposes, aims etc) of any proposed C^{3}I system.

The mission of any proposed C^{3}I system over its life-cycle must be stated at the outset. (Its purpose, after all, must have been known at its moment of conception!). The Mission must state the C^{3}I system's broad objectives and in particular the "how, when, where and by whom" it is to be used. The Mission Statement is then expanded into a set of broad requirements, which in turn are further refined into more detailed functional requirements. From these the C^{3}I system architecture and system specifications are derived and decided on.

An unclear, incomplete, or otherwise inadequate C^{3}I Mission Statement leads to incomplete, sometimes contradictory and even wrong requirements and, in turn, into a developed C^{3}I system with limited or wrong functionality, possibly implemented with an architecture which is not amenable to system expansion or corrective actions.

The boundaries and limits of each proposed C^{3}I system need to be delineated, and the following determined at the outset, for each system :

(a) The echelon (ie level) of command (National? HQADF? MCAUST, ACAUST, LCAUST etc? Or lower?)

(b) Strategic (ie national and relatively long decision cycles)? Or Operational? Or Tactical (ie localized and decisions more immediate)?

(c) Use to be restricted to war or conflict only? Or for peacetime operations as well (ie the management and administration of the ADF in peacetime as well)?

(d) Used for defence purposes only? Or include international commitments as well (eg. UN-type peacekeeping operations, or the class of operations undertaken with Allies in the Persian Gulf recently)?

(e) Used also for the ill-defined, "grey" areas of Defence/Civil operations (eg., natural disasters and the consequent emergencies; civil disorders; counter-terrorism; national counter-narcotics operations, such as aerial drug-interdiction etc)?

(f) To be manned and operated by the uniformed services only ? Or by civilians as well?

Lack of clear and complete C^{3}I missions and goals make the development and use of **C^{3}I measures of effectiveness (MOEs)** and other **C^{3}I evaluation criteria** difficult, if not impossible. (What do we measure and assess against what?). The outcomes of the application of MOEs determine the utility of the C^{3}I system, while during the development phase, their application will drive the direction and measure the progress to date, of the C^{3}I system. To compound matters further, C^{3}I system operators are generally sensitive to attempts to measure their individual performances, particularly if this is done by civilians.

Even when mission statements are unambiguous and clear, progressing to the next step pr new set of difficulties and uncertainties. This next step is the translation of these into C^3I req through consultation with the end user (or more comprehensively, with all the "stakeholders' who have influence over the development and acquisition process of a subject C^3I system (see below,, The term for this collaborative activity of converting and translating C^3I missions and goals into defined C^3I system requirements is **"eliciting and capturing (C^3I) requirements".**

Getting this right is a challenging and often frustrating undertaking, for three main reasons :

(1) Who the end-users are is often not at all obvious, even if the C^3I mission is well defined.

(2) The end-users or C^3I operators, who are one or two levels or more below the commander, articulate their needs, and hence requirements, based on their perceptions and in their natural language (by word, spoken or written, sketches, formatted document blanks, hand movements etc). These are often an incomplete and imprecise definition of requirements.

(3) When introducing new computer and other information-based technologies to improve and automate C^3I processes and systems, which hitherto have, in the main, been manual and personnel-intensive, the requirements and the associated processes will nearly always reflect the previous personnel-intensive processes and procedures; these, although perceived to be requirements, are often rather conventions only, matched to the previous man-intensive system. Not only may such conventions map poorly onto a computer-based C^3I implementation, but they may not be requirements at all, only perceptions of such.

However there may still be a need to avoid "deskilling" of manual procedures in operators when introducing and installing new automated systems. For example, **AUSTACCS** (see Section 7.3.1.5.b iii), the Command Support System for LCAUST HQ, specifically requires that "in the event of failure or lessening in efficiency of the automated system", AUSTACCS itself "facilitate a reversion to superseded manual operational procedures" **(AUS88)**; this of course will require operators to remain skilled in the "old" manual SOPs as well as become skilled in the "new" AUSTACCS SOPs..

It is therefore necessary that the end-user, during the Requirements Elicitation phase, recognises the essence of functionality, and distinguishes the difference between a "requirement" and a "convention".

The problems associated with eliciting and capturing C^3I requirements, and in particular distinguishing between conventions, embellishments, etc and functional requirements, is at the heart of many of the current problems associated with C^3I development.

4.1.3 Uncertainty Resulting from Multiple C^3I Stakeholders

There are many players, other than the obvious such as the "user", "developer", "funder" etc., who have important stakes in the development and use of a subject C^3I system **(REW89)**; these are called **"stakeholders".**

Stakeholders are those that affect a C^3I system, are affected by it, or both. They include the C^3I system proponents, the end-users, subordinates, data-sourcers, the funders, program managers, developers, builders, testers, maintainers, etc. Each has his viewpoint of the system and hence his perception what the requirements should be. In general, not all stakeholders are identified, and there is no formal mechanism to take cognizance of their legitimate stake in the development and life-cycle of a C^3I system. "Turf battles" and politics unfortunately often play a major part.

Unless mechanisms are developed and implemented that recognise the multiplicity of stakeholders, identify them, and reconcile (on a priority basis) their often different (but legitimate) perceptions of the C^3I requirements, conflicts will remain, resulting in incomplete, inconsistent, and often misunderstood C^3I requirements and all the consequent development and life-cycle problems.

4.1.4 Uncertainty over C^3I System Life-cycle

One of the few certainties during the invariably lengthy development, procurement, and in-service life of any C^3I system - which typically is of the order of 10-15, or more, years - is that **major changes will occur in :**

(a) **the threat**, with significant improvements in its capabilities due to technological developments;

(b) **national strategic priorities,** due to both domestic and external factors;

(c) **structure and size of the ADF;**

(d) **command and control structure,** at the single, uniformed Service level, and very possibly higher levels as well, to reflect (a), (b), and (c) above;

(e) **procurement budgets;**

and (f) **C^3I system capabilities,** driven by (a)-(d) above, as well as due to the developments in, and implementation of, new - and primarily Information Technology-based - technologies.

Although the actual nature of the above changes cannot be predicted at the beginning of the C^3I system life-cycle, the strong likelihood of their occurring must be accepted, consequently **mandating that any resulting C^3I system architecture must** lend itself to enable the C^3I system to **accommodate modification**, probably on a major scale, **and** certainly, **growth.**

The clearest trend is that of the impact of technology on the threat. Improvements to weapons and weapon-related sensors have resulted in stealthier signatures, longer ranges, shorter delivery-on target times, and greater precision and accuracy. The resulting impact on C^3I is that greater areas need be surveilled, consequently making greater demands on communications, on surveillance processing with more targets likely to be detected, and resulting in a larger tactical picture and assessment over a wider area; information processing is at smaller signal-to-noise ratios; and much shorter reaction and decision times are required. The changes to a C^3I system to accommodate these requirements include both significant information processing improvements, as well as growth, particularly in the Information Collection System and Intelligence and Information Processing Systems.

This, as well as the above, is more than the usual "motherhood" statement, namely, that .."C^3I systems will evolve as operational requirements change to meet new threats"...

4.2 Complexity of C^3I

Complexity manifests itself in C^3I in several ways :

(a) **Inherent C^3I system complexity**, since a C^3I system is itself a system of major (sub)systems, as listed in Section 3.3.2 above.

(b) **The difficulty and complexity of capturing the functionality of the C^3I end-user.**

(c) **A serious absence of a theoretical and intellectual base** for addressing C^3I in general, and C^3I architectures in particular.

(d) **C^3I is very software intensive**, a problem being compounded by the existing critical problem of the poor record, to date, of developing and delivering reliable, quality software for defence systems.

(e) **The customised, one-off nature of C^3I systems**, unlike that of other military and defence systems, which even if very complex are, in general, produced in quantity.

(f) **The two-sided, adversarial nature of C^3I** which must assume the presence of an intelligent enemy (or at the very least, an uncooperative one), with his own C^3I system, **with the resultant "information warfare"**, analogous to Electronic Warfare.

(g) **The geographical dispersal of the constituent C^3I (sub)systems.**

(h) **Technology advances in C^3I-"elated areas.**

4.2.1 Inherent C^3I System Complexity

Figure 3 showed a generic C^3I system, consisting of the five main (sub)systems, each complex in itself. Each of the (sub)systems consists of facilities, personnel, and specific Standing Operating Procedures (SOPs), as well as other procedures of custom or convenience. Consequently each system carries out a number of processes by multi-agent elements ie, by both humans and facilities, such as sensors and computers, work-stations etc.

C^3I spans a wide range of functional processes, from allocation of surveillance and sensors assets, the surveillance and detection processes themselves, information fusion from different sources and processes, data-base management, protection of information and intelligence, authentication of authorised users, decision and planning processes, distribution of intelligence and information, to communications network monitoring, and, if necessary, reconfiguration etc etc.

The number of disciplines and technologies involved is also wide-ranging and includes communications, information systems, information security, control, sensor and surveillance systems, software engineering, artificial intelligence, cognitive sciences, operations research, and above all, systems engineering.

4.2.2 Functionality of C^3I System End-user

The *functionality of the C^3I end-user* (the commander and the operators of the Command Support System, as well as the operators of the other C^3I (sub)systems) is key to its successful use. Eliciting these human element functionalities (ie gathering knowledge on end-user functionality and interaction with the C^3I system) from the end-user is a complex and challenging task.

The end-users, operators etc not only execute a number of specific SOPs, but also a number of individually customised, and non-standardised procedures. Indeed it is often argued that the successful commander is one who does not follow "conventional" SOPs, does not "go by the book", is unorthodox, and does the unexpected; this applies to his dealings with staff and very likely to the usage of his C^3I system. Intuition, initiative and individuality play key parts; different commanders balance these attributes of "command" differently with the other side of the coin, that of "control" (planning, organisation, reporting requirements etc). Consequently different commanders, and their staffs and operators, will have a different style, in particular in the way the C^3I system is used; for example a commander may insist always on more information requests from the SICS for greater detail in situation pictures, resulting in greater communication demands; he may insist on more options, in varying levels of detail; he may delegate more to some and less to others, with consequences on their workloads, and hence on the processing capacity of different workstations in the CSSs, and at different command echelons; etc)

Eliciting requirements from the end-users and operators, and transforming these into functions is complex, since what to a user may seem intuitive, does not often lend itself to clear articulation. Often the answer is " I'll know what I want when I see it!"

4.2.3 Absence of a C^3I Theoretical and Intellectual Base

A recurring theme at C^3I workshops, conferences and meetings is the acknowledged absence of a theoretical and intellectual base for addressing C^3I development in general, and C^3I architectures in particular, and the urgent need to redress this, specifically by developing, and ensuring the acceptance, of a mathematical C^3I Systems theory and discipline **(ATH87, DCA89, DCA86, MAY88, SOR89, VTR89).** Such a C^3I discipline would need to address, inter alia, the structure of a C^3I system (ie a C^3I "reference model"), its functional characteristics, and develop the tools, including appropriate **MOEs,** to design C^3I systems and enable their characteristics and performance to be evaluated.

It must be stressed that the shortcomings to date are not due to an absence of supporting C^3I technologies; rather there is the **need to develop and implement a rigorous C^3I systems engineering approach.** Thus,

> ..." the need for "systems discipline for C^3" ..(is) more crucial for success than the creation of new (C^3) hardware"... **(LYO86)**

This is yet again reconfirmed by one of the key findings of **(DCA89)** (another being the confusion in C^2 and C^3 terminology discussed in Section 2.1) that there is a critical need to establish "a mathematical discipline of C^2 Systems Theory". The lack of such appears to have had a significant impact in C^3I software development, in particular because without a systems approach, .."the inability to correctly formulate the (C^3I) problem"...would result.

Efforts are now underway to redress this in several defence R&D establishments, in (a few) US academic institutions under the co-sponsorship of key US DoD C^3I organizations and in the UK..

4.2.4 Software Development for C^3I

One of the key processes in C^3I are the collection and transformation of information into intelligence which, with other data and information already collectively integrated and interrelated (the existing "knowledge"), provides a "current situation picture". This situation picture is assessed and compared with previous situations; a number of possible responses are put forward: the optimum response is selected; a plan to implement it is drawn up; and then communicated to friendly forces for execution.

It is now feasible for many of these processes to be computer-aided or mediated, by updating and accessing specialised data bases, by using Artificial Intelligence (AI) techniques such as Expert Systems tailored for "most probable situation" generation, "similar past situations", "probable intent" etc, and for computer-aided mission and movements planning aids; as well as the more routine tasks of message passing, logging etc, networking of geographically dispersed computers and workstations, and data, information and human communications. This results in modern C^3I systems being very software intensive, specifically **..." as much as 80-90% of C^2 system costs have been estimated as attributable to software"...(DCA89),** which is significantly more than other software-intensive defence systems, such as new-generation aircraft avionics.

The current serious problems (and attendant "horror stories") with software development and delivery for defence systems is well known and acknowledged, and needs no further elaboration. The "obvious" solution to this is the application of Software Engineering, the objectives of which are to produce reliable, quality software through the following systematic approach :

(1) Problem Definition via "requirements elicitation" leading to Specifications.

(2) Planning the implementation via a Software Implementation Plan/Design.

(3) Implementing the plan.

(4) Testing and verifying the resultant software.

(5) Maintaining and managing the software over its whole-life.

The success of this systematic approach clearly rests on the accuracy, validity and detail of the requirements obtained, and the specifications derived from these. However a number of factors have been enumerated in previous Sections which preclude this, and result in incompleteness of, ambiguity in, and the inability, in general, to formulate properly, the C^3I problem and to decompose it into its component parts and requirements.

It follows then that the traditional approach to software development, based on a well defined problem formulation, does not immediately apply to C^3I systems. The lack of appreciation of this, and the need to look for, and implementing suitable, methods to overcome this problem, has been the major reason for the poor track record, to date, of delivered, working C^3I systems.

4.2.5 C^3I Systems : Only One or a Few of a Kind

The one-off, or a few of a kind, nature of C^3I systems provides its own set of complexities.

The data base for addressing development methodologies, as well as costs, is very limited, and in most cases, simply nonexistent. The same applies for addressing and estimating life-cycle costs.

There are no production runs. Prototypes are therefore harder to justify. Often the developmental model becomes the delivered, operational system. Testing of the kind well-understood and associated with weapons, or tanks or aircraft, is not applicable, and altogether on a different plane.

Yet because the C^3I process is generic (Section 3), and because C^3I systems are required to support the three operational commands (Land, Air, Maritime) and at different echelons of command as well, common processes and elements exist, even between such a small set of C^3I systems. For example: in the user-machine (graphical) interfaces; in the structure and organization of data-bases and their use; (multilevel) security implementation; networks and communications; and above all, in the commonality of architecture. Consequently opportunities exist, and can be taken advantage of, for reusing software elements at the module level, which perform the same, or similar, functions in the same, or in a different, C^3I system. The reuse, or rework, of software in existing C^3I systems for inclusion into newer generation of C^3I systems should also be explored.

4.2.6 Adversarial Nature of C^3I and Information Warfare

The nature of C^3I is "two-sided", that is, during conflict, a C^3I system is at the heart of operations against an enemy who must be considered intelligent and has a C^3I system himself, whether "primitive" or sophisticated. The successful masking of, and deception of an opponent about, one's own intentions often is the difference between success and failure in conflict. Consequently an enemy will not permit himself to passively suffer surveillance, monitoring and being reported on, but will deliberately, via a number of assets and actions, attempt to increase the uncertainty in the data and information being collected by the SICS of friendly C^3I systems, and consequently the uncertainty of the resulting tactical situation assessment. Alternatively he may try to reduce or eliminate surveillance information and other intelligence from reaching the C^3I system by jamming or physically and destructively targeting surveillance sensors, platforms etc, communication links, and other C^3I (sub)systems. (Even in peacetime, when a national/strategic C^3I system is monitoring what is designated as its strategic region of interest, potentially hostile, unfriendly, and neutral nations will practice, to a larger or lesser degree, deception and mis- or dis-information).

Current terminology for these activities is **"C^3 countermeasures"**, which is further divided into **"counter-C^3"**, which are measures taken to deny an opponent the ability to carry out effectively his C&C functions, and **"C^3-protection"**, which are measures taken by oneself to maintain the effeciiveness of own C^3I despite the counter-C^3 actions of the opponent. These terms are somewhat restrictive in that they do not contain explicit reference to "information" or "intelligence". As the activities encompassed by C^3 countermeasures are analogous to the tactics and techniques employed in Electronic Warfare, the term **"information warfare"** will be introduced to collectively describe them.

To account for Information Warfare will require greater complexity in C^3I systems. It will need to include the "obvious" requirement for C^3I System Security which will include multi-level security (MLS) across computers, software and communications; physical security by hardening, dispersal, mobility and redundancy; reductions in C^3I facilities' optical and signal emissions/signatures; and specific electronic countercountermeasures (ECCM) for signal, data, and information transmission and distribution. There is also the increasing need to provide C^3I system robustness and defence against a new, and increasing, repertoire of Information Warfare dangers (eg. computer viruses and worms, various forms of Trojan Horses ("trapdoors", "logic bombs") etc in software). In particular the susceptibility of the newer proposed C^3I systems to these dangers is likely to be encouraged and enabled by C^3I architectures which will be increasingly make use of:

(a) computing and communications facilities compliant with Open Standards, ie non-vendor specific, commercial-off-the-shelf facilities, hardware and softwar? (section 6.1.2.7);

(b) civil sector or commercial communications such as the recently introduced Integrated Services Distributed Network (ISDN), and its follow-ons, between C^3I subsystems and nodes, and other existing bearer links (section 6.1.6);

(c) digital data transmission and processing.

This is because of the increasing use of, and easier access to, world-wide distribution (and eventually full world-wide compatability of) the commercial/civil sector communications infrastructure for data and multi-media information transmission to all and sundry who are prepared to pay the existing commercial access and usage/rental rates.

4.2.7 C^3I Systems as Distributed Systems

C^3I (sub)systems and nodes are generally geographically distributed. This is dictated by the demands of dispersing surveillance sensors and information collection assets to maximize the area of surveillance in general, and to survey specific areas and regions of interest, in particular. It is dictated as well by the nature and capabilities of the opponent's surveillance and weapons (range, speed, homing-on-C^3I system-emissions/signatures etc) targeted against the C3I system. Dispersal enhances survivability.

This, together with various C^3I functions which by their nature are interdependent, distributed and occur simultaneously (eg data/information processing, operator activity, communications), lead to requirements for distributed processing and system control, with all the complexities and problems attendant to distributed architectures.

4.2.8 Technology Advances in C^3I-related Areas

The typical current rate of advance in technology is such that a major technological advance in most fields is expected every 3-4 years. This is particularly true in the C^3I area which is very dependent on Communications and Information Technologies, two areas heavily driven by commercial pressures and market incentives.

The development and procurement phase of a major defence system, such as a C^3I system, is typically of the order of 10 years or more, during which period at least 4 to 6 major technology changes may be expected (counting communications and information technology as two distinct fields). During the expected 15-20 years of in-service operation, another 12 or so changes may occur as well resulting in anything **up to 20 major technology changes likely to occur over a C^3I system's whole life-cycle!**

These changes, being much more rapid than system development and procurement, often result in obsolescent, even obsolete, C^3I systems being fielded. Consequently the demand from program managers during development, and later on, from users/operators or C^3I system whole life-cycle managers, for upgrading their C^3I systems and incorporating such technology advances will be inevitable. Such rapid advances invariably go hand-in-hand with significant reduction in computing costs, which in turn promotes, and makes possible, a "throw away-and-replace" attitude for terminals, work stations, and the like. Such rapid replacement, together with the nature and usage of the C^3I (sub)systems, in turn, will put pressure to examine and reassess the requirements for compliance with MILSPECS (and possibly even ruggedization for fixed-site, high level C^3I facilities). If the requirements for MILSPECS can be significantly relaxed, this would further encourage this "throw away-and-replace" philosophy, making Commercial-off-the-shelf (COTS) procurement possible, even inevitable.

However, since several major technologies are involved in C^3I, such advances will not always necessarily match or complement each other. Incorporating what may seem to be an "obvious" technological improvement may not realise its full capability in the C^3I system, since the total system capability or performance limit may be imposed by another technology in the system running at its limit.

Unless such tools as C^3I system mathematical models, simulation, MOEs etc are available and sensibly used, any such proposed C^3I system "improvements" will not only result in disruption in the development and procurement phases, very likely at considerable expense, but possibly with marginal improvements in performance only, if at all.

4.3 Consequences of Uncertainty and Complexity on C^3I Development

It is clear from the above that the analysis, design, development and acquisition environment for C^3I is fragile, uncertain, complex, and even hostile.

Most of these uncertainties and complexities are organic to C^3I, while others are due to the inevitable advances in technology, the nature of current defence systems development and acquisition, as well as due to the periodic changes to key ADF personnel, and the less frequent, but critical changes to national and ADF structures and objectives.

The traditional development and acquisition sequence applicable to more conventional, multi-unit production defence systems, namely : identification of requirements; feasibility studies; concept validation; definition studies; specifications definition; full-scale engineering development; testing; production; testing and training; life-cycle maintenance and support; is not applicable immediately, if at all, to C^3I systems. (Although this has not stopped development and acquisition of such under this traditional approach, with not unexpected results and with all the attendant "horror" stories).

It follows that a new strategy, using an appropriate set of tools and methods needs to be found, developed and adopted, for the development and acquisition of C^3I systems. That strategy is one of **gradual, or evolutionary and incremental development and acquisition.**

5 C^{3}I Evolutionary Acquisition

5.1 Evolutionary Acquisition

Evolutionary Acquisition (EA) of (C^{3}I systems) is based on the ..."**analyse-a-little; fund-a-little; build-a-little; test-a-little; field-a--little".. principle.**

It specifically applies to, and matches optimally, systems whose requirements evolve with time, whether due to incomplete specifications ab initio, or because of evolving command and Force structures, or rapid advances in relevant technologies, as well as for system development in times of uncertain funding.

It is worthwhile to quote the definition of EA, accepted by both the (US) Defence Systems Management College and by AFCEA ((US) Armed Forces Communications and Electronics Association, a professional body whose main interest is C^{3}I) (quoted in (**CUL88**)):

> **Evolutionary Acquisition** is an acquisition strategy which is used to procure a system expected to evolve during development within an approved architecture framework to achieve an overall system capability. An underlying factor in evolutionary acquisition is the need to field a well defined core capability quickly in response to a validated requirement while planning through a "block" upgrade program to eventually enhance the system to provide the overall system capability. These increments are treated as individual acquisitions, with their scope and content being the result of both continuous feedback from Developing and independent Testing Agencies and the User (Operating Forces), and the desired application of new technology balanced against the constraints of time, requirements and costs.

"Evolutionary development" is an integral part of "evolutionary acquisition" in C^{3}I, and is the development content of the EA process as defined above, being its .."analyse-a-little..build-a-little..test-a-little"..component.

This definition of EA, it must be noted, applies to **systems**, and increasingly through usage, to C^3**I systems and their component subsystems, over their whole life-cycle.** EA is also being increasingly applied to large software development projects, where some differences apply to the meaning of certain EA associated terms (and within which, for well-defined blocks of the software, other acquisition processes, including those based on the traditional "waterfall" model, are permitted).

The process, shown in **Figure 4**, requires an existing fielded system, or one developed with some basic or "**initial operating capability**" (**IOC**) based on an initial set of requirements, which may be called the "**baseline system**". The process begins when requirements are further refined or additionally defined; a number of these new requirements are aggregated and then tested via simulation and/or on C^{3}I testbeds as well as field-tested during exercises to validate them, determine their utility, and assess their cost benefit. The C^{3}I system is then upgraded by that **increment of approved, cost-beneficial requirements**, and **funded as a new acquisition,** with the process cycle typically being on an annual basis or, more likely, at intervals between major (C^{3}I) field exercises.

As shown on Figure 4, the process iterates over six steps :

(1) collect refined, evolved, or additional requirements from user (and other stakeholders);

(2) at some point in time, obtain authorization from key stakeholders (ie those with "voting rights") that the subject requirements collected to date are "needs" and not "wants" and establish traceability of each to C^{3}I policy, doctrine, operational requirements etc; continue, as a parallel activity, further collection and refinement of requirements;

(3) test and evaluate effect of authorised requirements on system performance and effectiveness via simulation or on a C^{3}I testbed and assess the cost-benefit;

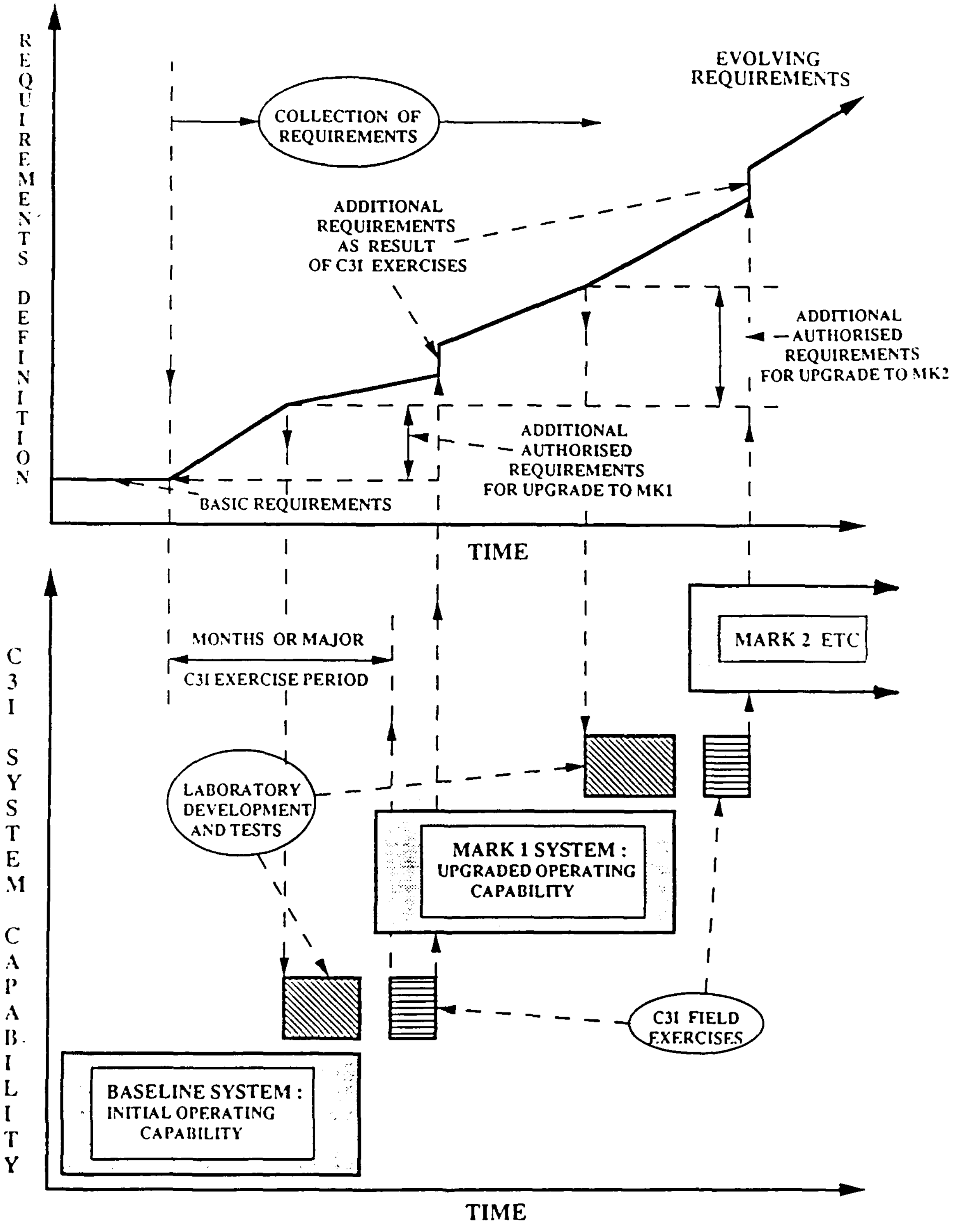

REQUIREMENTS DEFINITION
COLLECTION OF REQUIREMENTS
EVOLVING REQUIREMENTS
ADDITIONAL REQUIREMENTS AS RESULT OF C3I EXERCISES
ADDITIONAL AUTHORISED REQUIREMENTS FOR UPGRADE TO MK2
ADDITIONAL AUTHORISED REQUIREMENTS FOR UPGRADE TO MK1
BASIC REQUIREMENTS
TIME
C3I SYSTEM CAPABILITY
MONTHS OR MAJOR C3I EXERCISE PERIOD
MARK 2 ETC
LABORATORY DEVELOPMENT AND TESTS
MARK 1 SYSTEM : UPGRADED OPERATING CAPABILITY
C3I FIELD EXERCISES
BASELINE SYSTEM : INITIAL OPERATING CAPABILITY
TIME

Figure 4. Evolutionary Development and Acquisition Process

(4) via new funding and acquisition, implement the increment of approved changes on the C^{3}I system with Initial Operating Capability (IOC);

(5) field-test via exercises (ad hoc, annual or major C^{3}I exercises);

(6) field system with beneficial incremental changes as "Upgraded Operational Capability"(UOC);

(7) repeat cycle again.

Evolutionary acquisition has in recent years been adopted by several US Commands and NATO as the strategy by which C^{3}I systems need be developed and acquired **(CUL87, CUL88, DIE90, SHO90)**. Some 8-10 C^{3}I projects procured under EA have proved the strategy; a detailed case history for the US Army Europe Command and Control System (UTACCS) is given in **(GIO91)**. **(HEN91)** further expands on EA, with reference to the procurement of Command Support and Military Information Systems, and Project JP2030 in particular.

5.2 Benefits of Evolutionary Acquisition

The following are the key benefits of adopting the EA strategy to the C^{3}I system and their users:

(a) EA lends itself to new systems, or it can be grafted onto existing C^{3}I systems or subsystems (architecture permitting for the latter two).

(b) A working C^{3}I system with some core operational capability of its intended capability is in the field at any point in time. This is to be contrasted with the conventional development and acquisition process of developing a system on the sidelines at great cost, over a lengthy period of time (years), and with the eventual user's patience being lost and replaced by frustration and even dissatisfaction. (Instances are known where user frustration has led them to improvise their own C^{3}I solutions with personal computers and COTS software.)

(c) System capability grows over time increments of months, rather than years.

(d) Close cooperation between the end user, developer, tester and sponsor is a key ingredient to the overall success. The developer understands the user's requirements better which is in turn reflected, at the end, in a system much closer to the user functionality, than if the system had been specified in isolation. The user on the other hand gains a better appreciation of the possibilities offered by technology, as well as seeing the results of his inputs. User participation in EA and his early exposure to it works for better acceptance of the delivered system at the end.

(e) The increase in system capability is due to direct feedback between user, developer, sponsor and tester (often the tester is also the user). The process eliminates information buffers; the true user, rather than the "nominal user", such as the "acquisition authority" or even the "R&D authority" under the conventional acquisition process, is involved to articulate his real requirements to the developer. Synergism is created between the participants during the development phase. Only successful changes are incorporated into the system. A corollary to this is that the chances of gross mistakes (which, when they do occur in conventionally developed and acquired systems, tend to surface close to, or at the system integration stage ie near the end of the development phase) are eliminated.

(f) EA excludes the premature (or rather more likely delayed!) introduction into service of large, untried C^{3}I systems, which, from past (overseas) experience are generally over budget and behind schedule.

(g) System obsolescence, characteristic of systems developed by the current conventional process is minimized, possibly eliminated under EA.

(h) EA does not require large upfront budget outlays. By its nature the spend is phased. A corollary to this is that large budget overspends are eliminated. (Evidence suggests that, in fact, significant savings occur).

(i) EA inherently allows growth, extendability and modification, catering for one of the few certainties in the uncertain area of C^3I, namely that over time even a well-defined and specified system will grow and require modification to reflect changes in operational requirements due to the changing threat.

(j) EA exploits and is leveraged on developments in technology in the commercial sector, since C^3I is heavily dependent on Information and Communications Technologies. This applies not only to products, but also the vast R&D resources of the civilian and academic sector contribute to C^3I developments, instead of only the (significantly smaller) R&D resources of the Military/Defence sector.

(k) The non-sequential process of EA lends itself to parallel activities of requirements collection and definition; analysis and design; development; testing; and implementation.

(l) The phased approach of EA will permit advantage to be taken of ongoing and near-term developments in the high-priority area of the science of, and systems engineering of, C^3I.

(m) Finally, **EA is the process by which the C^3I Migration Plan is to be effected.**

5.3 Problems Facing EA

Traditional and current practices of project management, development and acquisition require the upfront definition of system requirements and specifications, together with funding approval in several well defined phases or in toto.

Recently, a senior member of the US Packard Commission on Defense Management, inter alia, stated **(STA90)** :

> " the (current acquisition) system...is flawed in fundamental ways...It's flawed at the very beginning in determining the so-called requirements of a system, in that (it) deliberately isolates the requirements process from technical and program realities".....

EA has been developed - and successfully applied in the US and other Western/NATO countries - as a response to this, in particular to C^3I systems with their inherent uncertainties and complexities. It works precisely because it runs counter to traditional and current development and acquisition practices. Its acceptance by procurement authorities within Defense, as well as by the stakeholders in ADF C^3I systems, current or future, will need a change of heroic proportions in the current processes, attitudes and mindsets; in fact a wholesale change in the current "acquisition culture". Such a change will not be easy, nor will it be overnight.

The prevailing concern seems to be the misconception that EA would require an almost open-ended, loosely controlled budget. In fact, management controls are probably tighter under EA, since the allocated spend for the "total" C^3I system is not approved upfront (as under current acquisition procedures), but consists of a number of very much smaller acquisitions with associated smaller spends, each treated and authorised separately, with each acquisition being for an aggregate of C^3I system capability upgrades agreed to by the C^3I system stakeholders, who by definition, have the wellbeing of the system being developed and acquired at heart. A key reason why EA has been successful in delivering C^3I systems, is that the acquisition process, particularly its management and associated controls, requires the involvement of the C^3I system stakeholders, rather than, as hitherto, been limited to, and managed by, bureaucracies separated from the problems and realities of the technical, developmental and user communities.

(HEN91) makes some very useful recommendations regarding the adoption of EA by Defence.

Most likely, as well, **the management of C^{3}I, and in particular the implementation of the C^{3}I Strategic Plan, will need to be evoiutionary.**

5.4 EA and Prototyping

Prototypes and prototyping have been associated, but occasionally confused, with Evolutionary Acquisition; it has even been suggested as an alternative acquisition method **(SHO90).**

Three distinct kinds of prototypes have been used for C^{3}I development, each with a distinct role :

(a) rapid or exploratory prototypes;

(b) experimental prototypes or test-beds;

(c) evolutionary prototypes.

A useful summary on prototyping, albeit for software development rather than for C^{3}I, is **(JON90).**

5.4.1 Rapid or Exploratory Prototypes

"Rapid" or "exploratory " prototyping is a tool for promoting dialogue between end-users and developers, and as a focus, for quickly exploring and eliciting user C^{3}I requirements, in particular during the stages of the user having difficulty in articulating his requirements; it is the best tool in cases when the user states "I'll know what I want when I see it".

The "prototype" is a sequence of interactive, animated computer displays ("animated story-board") which, through a set of "canned" scenarios, the developer presents to the end-user the "look-and-feel" of the real system (as the user would see the system). The interactive displays may be, say, of an enemy ORBAT superimposed on maps of an area of operations, on which the user may wish to window and zoom in on some particular area and seek more information such as (enemy) Unit name, composition, capability, readiness status, etc. Through such initial displays, a dialogue is established between user and developer in the medium of the end product, as far as the user is concerned, namely that of user-system computer interfaces. User actions and responses are recorded and used as the basis for making changes to the "storyboard"; sessions are repeated until the user is satisfied.

Prototyping in this fashion is often rapid - hence the term - and very affordable, as many Commercial-off-the-shelf (COTS) software tools exist (developed for other, non-defence applications). **(OVE89)** provides a good overview, assessment and cost of these tools.

Such prototypes are often "throw-away", as they model a very limited portion of the C^{3}I system, essentially being scale models of the C^{3}I user interface, without underlying functionalities and lacking many (software) "quality attributes" (such as reliability, portability etc). However when approved by the user, they are, in that instance, a valid model for at least the system man-machine interface and the type of information in user required formats, and hence **they are a form of specification** ie the prototype, or rather the source code generating it, is the specification and should be used for that purpose.

5.4.2 Experimental Prototypes and Test-beds.

Experimental prototypes are those on which C^{3}I requirements are further developed, achievability or otherwise is proved, benefits are assessed, and implementation into fielded systems is explored and designed.

Another, more common, name for such prototypes is **(C^{3}I) testbeds.**

Such C^{3}I testbeds are more in the class of formal laboratory-type facilities, where developers and end-users jointly participate in the exploratory development of proposed enhancements to existing systems, particularly to test new concepts. However testbeds may have a rapid prototyping capability as well. For meaningful and realistic R&D experimentation, testing and evaluation of a C^{3}I systems, all C^{3}I (sub)systems need be represented, either by software or hardware simulation, or both, to provide a sensibly credible environment required for results and conclusions to be valid.

Such testbeds/experimental prototypes can emulate, explore and evaluate proposed C^{3}I structures, configurations, and architectures, as well as specific improvements, enhancements and responses to refined requirements, and, in particular, to test new C^{3}I system and applications software.

(DCA89) heavily pushes the need for, and the setting up of, such exploratory prototypes/testbeds as one of its major recommendations to advance the progress of C^{3}I (its other major findings already mentioned were the urgent need to develop a science of C^{3}I, and the need to clarify the existing confusion in C^{3}I terminology).

5.4.3 Evolutionary Prototypes

This class of prototype is the case where an existing operational C^{3}I system is taken as the baseline system and is gradually adapted and evolved into a more capable system by the incorporation of new or better defined or refined requirements. The resulting system thus becomes the design for the improved and more capable operational system.

Because C^{3}I systems are built in one- or two-offs, the upgraded "prototype" may, in fact, become the more capable, fielded system.

5.5 C^{3}I Life-cycle Support System (LCSS)

It is clear from the foregoing that evolution and growth of a C^{3}I system occurs over its whole-life cycle. It is therefore not only prudent but also necessary to set up a **C^{3}I Life-cycle Support System (LCSS)**, an entity organic to a C^{3}I system, and for it to be the fifth major (sub)system of a C^{3}I system. Its main role would be to manage and implement the evolutionary C^{3}I system development, growth and maintaining capability with the evolving threats and evolving ADF command and Force structures.

Being a system, it will require to have :

(a) missions and objectives;

(b) facilities;

(c) personnel;

(d) support and funding.

5.5.1 Missions and Objectives

The mission of the LCSS is to be the centre of excellence and expertise for the development and implementation of C^{3}I systems for the ADF, and to plan, manage and implement the Transition/Migration of current and existing C^{3}I systems to the envisioned C^{3}I systems.

In particular, its objectives include :

(1) proposing organizational structures, and developing and implementing methodologies, which will assure that the current and foreseeable developments of ADF C^{3}I systems are in accord with user and stakeholder requirements, and are traceable to C^{3}I policy and doctrine;

(2) the responsibility for eliciting and gathering C^{3}I requirements from all stakeholders, transforming approved and authorized requirements into functions, and investigating, implementing, and integrating them into C^{3}I systems;

(3) developing methods and techniques for C^3I measures of effectiveness and other C^3I system and subsystem evaluation criteria and evaluating the benefits of proposed requirements, changes, enhancements etc, so as to steer the incremental development of C^3I systems;

(4) developing, maintaining and improving as required, mathematical and physical models and simulations to investigate and predict C^3I system behaviour and performance, and validate concepts; and in particular developing and operating a C^3I testbed for this purpose;

(5) encouraging and maintaining dialogue and interaction with all C^3I stakeholders, through the use of, and interaction with, their facilities, including for user training and development;

(6) interacting with C^3I stakeholder committees and other Defence Committees so that C^3I development momentum is maintained.

5.5.2 Facilities

The LCSS facilities should include the following :

(1) A computer-based environment analogous to an IPSE (Integrated Project Support Environment) to manage C^3I system development, and in particular to manage and assure traceability between C^3I system requirements and functions and C^3I policy and doctrine (see sections 6.1.2.3 and 6.1.2.4). An IPSE is an integrated set of system development tools covering the specification, design, programming, building and testing of computer-based systems, and thus includes any CASE (Computer Aided System Engineering) tools for software generation.

A useful overview of the categories of software development environments currently in development or available is in **(DAR87)**, while a concept for a process - in the industrial sense of mechanising the steps - for developing large software-based systems, based on object-oriented methods (Section 6.1.2.1), is given in **(JAC91)**.

(2) A reconfigurable C^3I testbed for exploratory development and experimentation, for testing and assessing changes, improvements etc, in particular, to systems and applications software, and to explore C^3I structures and architectures.

(3) Analytical, modelling and simulation tools and facilities to support the above.

(4) Facilities and tools for user requirements elicitation, user-C^3I system interaction, and user training.

5.5.3 Personnel

Professional and technical staff drawn from, as well as facilities existing in, the Information Technology and Communications Divisions of ERL/DSTO can be organised to form the LCSS. Appropriate staff from HQADF, the user community and from other stakeholder organizations should be attached to the LCSS on a shorter or longer term basis. Staff exchanges and attachments with, and from, other allied nations (through the various existing civilian scientist/engineer and uniformed Services exchange agreements) should be pursued.

5.5.4 Support and Funding

The success of developing, implementing and maintaining ADF C^3I systems will depend on an effective LCSS. It must therefore have the support of all C^3I stakeholders and be funded appropriately.

It is recognised that a LCSS will not be formed, nor reach maturity and full capability, overnight. It will need to evolve to those levels by stages, thus being subject to evolutionary development itself, and can be funded in a like, evolutionary and incremental, manner.

6 Technologies Enabling C^{3}I Evolutionary Development

How well do existing technologies support C^{3}I in general, and evolutionary acquisition and its associated evolutionary development in particular?

The purpose of this and the following Section 7 is to indicate the state-of-the-art, scope and, in most instances, the maturity of these relevant supporting technologies and to show that, in the main, no major technical risks are anticipated. Details of how specific tools are used to solve particular C^{3}I problems are deliberately avoided, as this is out of place in a report of this nature.

First, the tools and techniques available to support the critical activity of C^{3}I software development are described, followed in Section 7 by tools and methods applicable to the development and implementation of the separate C^{3}I (sub)systems. Other tools commonly used in the C^{3}I field include mathematical modelling and computer simulation as well as various man-in-the-loop simulations including wargaming; these will not be covered here.

6.1 C^{3}I Software Development Tools

Any software development environment, tools and techniques for C^{3}I, as well as any resultant C^{3}I software architecture must take account of, and accommodate, the following requirements :

(a) C^{3}I is synonymous with a large and complex software development project.

(b) C^{3}I implementation must be by evolutionary development due to: initial incomplete requirements definition; requirements which over time become better defined or redefined; and to accommodate systems growth and capability extendability.

(c) The C^{3}I system is a distributed network, with many concurrent activities.

(d) Interoperability of ADF C^{3}I systems between different echelons of command and lateral commands (including C^{3}I systems of Allies) is required.

(e) Implementation should be, wherever possible, with commercially available (commercial-off-the-shelf (COTS)) equipment, in accordance with **(FSR91)**.

(f) The C^{3}I system whole-life cycle will typically be a minimum of 15-20 years.

(g) **Ada** is the preferred programming language. Although not mandated for use in ADF weapons and systems, its use is mandatory by US DoD and NATO.

(h) Network and systems software security, commensurate with the high and multi-level security of C^{3}I systems, is required.

(i) As a consequence of items (a), (b), and (d), software re-use is highly desirable.

Two strategies for developing the software for C^{3}I systems suggest themselves :

(1) acquire, and exploit, existing successful C^{3}I system and applications software developed commercially and consistent with evolutionary acquisition and development methodology, and together with its associated development tools, "fine-tune" or customize it to ADF requirements using the existing C^{3}I baseline system; or

(2) acquire tools and develop C^{3}I software ab initio, for existing ADF C^{3}I baseline systems.

Both approaches are currently viable.

6.1.1 Customizing Commercially Developed C^3I Systems Sof‡ware

Several successful C^3I systems have been developed and acquired under EA in the US anu NATO countries (**CUL88, DIE90, GIO91**). One specific project, developed commercially by TRW and partly funded under Independent R&D, is the Command Center Processing and Display System Replacement (CCPDS-R) (**ROY89**), which has been successfully fielded to higher level USAF Commands.

Its key features include :

(a) It is based on object-oriented methods, using a predefined set of logical network objects and a predefined set of operations, resulting in a "Network Architecture Services" product, which is then used to construct real-time networks, which support "flexible, open architectures".

It is C^3I -specific and applicab!e to large distributed multi-task networks.

(b) Its architecture uses re-usable software building blocks, programmed in Ada. These software blocks have well-defined behaviour and interfaces.

The software is thus highly re-usable.

(c) It is currently limited to DEC VAX VMS networks, but efforts are under way (1989) to provide heterogeneous (ie multi-vendor) capabilities.

The Network Architecture Services (NAS) concept has both technical and commercial features which may lend itself to be used as a C^3I software architecture skeleton and which could be adapted and evolved into C^3I systems (or C^3I (sub)systems) for the ADF.

The disadvantages, however, are, firstly, that it is a proprietary system with the potential for, and disadvantages of, single-vendor "lock-in" and, secondly, it has yet to have its potential open-systems and heterogeneous capability demonstrated.

However developments of this nature, both in the (overseas) commercial area and in the government defence sector (of Allies) need be monitored, not only for the "lessons learned" regarding C^3I EA, but also for possible procurement and eventual adaptation for ADF C^3I systems

6.1.2 C^3I Software Development Methods and Tools

Any software development tools and methods which are to produce software for C^3I must not only result in software and code so structured that it is robust to changes in requirements and functions, but result in **quality software** as well.
Software, to qualify as "quality", must have the following attributes (**MEY88**):

(1) **correctness** ;

(2) **robustness** ie retain functionality or gracefully terminate in abnormal operating conditions;

(3) **extendability** ie the ease and ability with which it may be changed to account for modifications in its functional requirements;

(4) **reusability,** in part or in whole, for new applications;

(5) **compatibility**, the ease with which it may be combined with other software products);

(6) **efficiency** ;

(7) **portability,** the ease with which it may be transferred to other, different hardware and software environments;

(8) **verifiability** ;

(9) **integrity** ie secure against unauthorized access and modification;

(10) **ease of use**.

6.1.2.1 Object-oriented Software Development

Much of recent software development, programming and coding, has been by what may be loosely called **"structured"** or **"top-down"** design and programming. This is essentially a **procedural approach** to programming, with the computational process being considered as the sequential execution of a list of tasks. It is predicated on the assumption that problems, tasks, processes etc, which need to be programmed, are well-defined and bounded, and can be hierarchly decomposed into functions of ever greater detail. This software development approach tends to reflect - at various levels of abstraction and through the use of procedures operating on data - the operation of the computer platform, rather than reflect the problem or the application being modelled.

Such a methodology does not support evolutionary development, specifically software extendability. A change in functionality, or in data format, often seemingly trivial, can ripple through the tightly connected branching structure that is characteristic of this design and programming methodology, resulting in program redesign and reprogramming not commensurate with the changes causing these. Software configuration management and control ie keeping track of, and documenting, all the software changes in the various fielded systems, can be and, more often than not, is a nightmare.

A **new software development paradigm** which supports the evolutionary approach, and is now heavily promoted for software whole life-cycle management and maintenance in general (after all during the whole life-cycle, changes, some major, are to be expected in any software-based system, not only to C^{3}I systems) is the **"object-oriented" method** (O-OM) **(BOO86, MEY88, HEN90, AND90,** inter alia).

The **O-OM** paradigm is a partial outgrowth of **modularity principles** in programming design and coding **(MAR91)**. Here programs consist of interconnected modules, each of which performs a number of logically related tasks. Internal implementations are not "visible" externally ("information hiding"). Communications between modules, during execution, is via well-defined "interfaces"; internal module changes can be made without affecting the interfaces, because of the aforementioned information hiding. Moreover, modules are compiled separately and individually. The latter feature, together with information hiding, enables changes to be readily made to modules, localising any ripple effects. Large problems can thus be broken into more manageable pieces, and delegated to different programmers.

O-O programming methods are more than just the use of modularity principles. O-O methods are a new problem analysis, design and programming paradigm based on organizing the problem and resulting software program, not around actions and tasks as in the hitherto orthodox procedural, structured top-down approach described above, but around the data to be processed, or, more correctly, around the **"objects"** which are to be manipulated. O-O methods stress the definition and representation of objects in the real world; these "objects" possess certain **attributes** and specified **services** (tasks etc) which are associated with these.

Objects are the constants in any system or process (in C^{3}I objects may range from a surveillance sensor, to a specific file, or a graphic user-machine interface, or an enemy Orbat, or even a C^{3}I functional products eg. "target Y location"). Procedures, functions etc, may change, but objects remain, even if their "attributes" are changed or augmented, and if their interactions ("services") with other objects change. Reorientating system analysis, design, and programming along objects, and away from functions and tasks, leads to a more stable ("robust") system process. During evolutionary development, as a C^{3}I system changes due to better analysis and understanding, or due to demands for increased capability, the relationships, functions, and dependencies change, but the objects on which they act on, remain. Objects may, of course, themselves be changed, or additional ones created, but any rippling effects remain localized.

For C^3I applications, the O-O approach is to partition the proposed C^3I system and its functionalities into **objects** which become the basic modular units during the **C^3I analysis, design, programming and testing** phases. An **object** has a **name**, specific **attributes**, and has **services** performed on it by, and requested by it from, other objects. Program implementation is by passing **messages** between active objects, which invoke **methods** that manipulate those objects.

The particular benefits of O-O methods to C^3I are :

(1) It specifically supports and matches excellently **evolutionary development** (via **open/closed interfaces** and **inheritance**).

(2) It encourages the extension of existing code and **software re-use** (via the properties of **polymorphism** and **inheritance**).

(3) It results in **very compact code**, in the sense of a significantly smaller number of lines of code compared with more traditional approaches (via **information hiding/encapsulation, polymorphism** and **inheritance**).

(4) Since O-O methods include **O-O analysis, O-O design, O-O programming** and **testing,** we can talk of an **O-O system development life cycle (HEN90)** with 1:1 mapping between these development stages, with the result that "**seamless**" transitions and handovers between these phases result. It is the problems occurring during the handover between these phases that so bedevil the software development cycle when a variety of analysis, design and programming methods are used. Consequently, through the common O-O approach, C^3I analysts and system designers can follow O-O programs more easily, while programmers can follow analysis and design in a similar fashion, and at higher levels of abstraction.

(5) It supports programming in parallel by a team of programmers.

The three main broad areas of application for O-O methods in C^3I are :

(a) C^3I system modelling and simulation (for performance modelling; system effectiveness evaluation ; assessment and evaluation of proposed changes; etc).

(b) C^3I systems support software (graphics user-machine interfaces; multi-media data-base management; multi-level security; C^3I network control; network reconfiguration; etc);

(c) C^3I applications (specific data-base applications; situation assessments applications based on maps/geographic information systems; decision and planning support aids; etc).

Ada, while not a true O-O language, does support and lends itself to O-O methods **(BOO86, BOO87).**

A strong advocacy for using O-O methods for C^3I system development directly has been recently reported **(AND90).**

6.1.2.2 C^3I Software Life-cycle Management Tools and Techniques

A fundamental shortcoming, even flaw, to date in the software production life-cycle is that the conversion of a requirement into a specification and, in turn, its conversion into a software implementation, is informal and, generally, undocumented (**GRE83**). In software maintenance and development, whether as a result of requirements being refined, redefined, or added to, the information and the rationale behind each software programming change or step already in place, is not generally available during the later maintenance phase. For C^3I, in particular, such changes to requirements, specifications and programs are the rule, not the exception.

The shortcoming in software developments to date, has been the absence of a technology to support these numerous and knowledge-intensive activities that constitute that critical phase of the software development process, in particular the conversion of requirements to specifications to software implementations. Not only must tools to support this be developed, but the software development process paradigm needs be changed to explicitly report and support these knowledge-intensive processes (**GRE83**).

The above is one particular but key, from the viewpoint of C^3I software development, aspect of the general problem associated with software development, which, in the past 10-15 years, has led to the development and application of "software engineering" methodologies.The basis of software engineering is the application of the control principles of engineering practice to assure quality software as the end product of software development. To this end, a class of products, based on the application of computers to the process of software development, called **CASE tools** (Computer Aided Software Engineering), have been developed. These tools include :

(a) **Fourth Generation Languages (4GL)**. These include :

(1) "declarative" or "non-procedural" languages, which permit programming at a "higher" level, by stating what result is required, rather than how this result is to be obtained, as required with the more conventional "procedural" languages; and leading to a significant reduction in the number of source code statements;

(2) special purpose packages such as spreadsheets, dBase, and database management tools;

(3) "applications/program generators" which generate source code of applications programs from descriptions of the problem, rather than from detailed programming.

(b) **"Information Engineering" (THO87, MAR90, RIC91)**. This is a newly emerging methodology generally based on a number of semi-proprietary CASE tools for implementing large Information Systems. Its objectives as well as the process is described by the following **(THO87)** :

> ...Information Engineering develops sound, integrated information systems....by using an engineering process to determine objectives and requirements, to specify and analyze designs, to prototype products before production, and to manage the process by objectives, costs, and schedules...

In essence it uses a "total enterprise", top-down approach of examining an (usually business/commercial) enterprise, its mission, strategic objectives, structure and organisation, decision-making processes and information structures and flows, and through the use of computer -aided and -mediated applications and tools on the resultant knowledge of the subject organisation, permits (computer-based) informations systems to be developed which support the mission, objectives, decision processes, and day-to-day operations of that enterprise. Key to its success is the development, acceptability and use of standards, and in particular the development of reference models on which to develop such standards and with which tools and the processes to produce the resultant information systems comply with. Information Engineering offers much promise and is maturing rapidly (**MAR90**).

(c) Proprietary CASE tools representing particular aspects of the Information Engineering approach and exemplified by **JAD** (Joint Applications Design) and **RAD** (Rapid Applications Development) (**MAR90, AXI91**), used in conjunction with other CASE tools. From the limited information available, the current applicability of these tools is for the development of relatively small, new applications (with perhaps poorly specified requirements) on an existing commercial computing environment.

It is outside the scope of this Report to go into any detail of these CASE tools. Rather the following tools and techniques, which are either C³I-specific or very pertinent to C³I and are currently in development or in use, will be briefly described here :

(1) **KBSA** (Knowledge Based Software Assistant) ;

(2) **CUBE TOOL**;

(3) The technique of **Exploratory Prototyping.**

6.1.2.3 Knowledge Based Software Assistant (GRE83).

The objective of KBSA, currently being developed in the US, is to provide an automated means of capturing, and reasoning, about software development activities, during the software development and maintenance phases ie when software requirements and specifications change.

The KSBA will automatically document the occurrence of every requirements input and programming activity, ensure their proper sequencing, and coordinate the activities of software development staff. Initially it will form a **computerized corporate memory**, in the face of inevitable staff turnover, by demanding and recording the rationale for each activity in the software development process, **in a machine-readable and manipulatible form**. For C³I applications, this would need to include the traceability of every "requirement" to an appropriate authority, based on approved C³I policy and doctrine pertinent to the missions and objectives of the subject C³I system.

Progressive and incremental developments of the KBSA, based on AI/knowledge-based methods, aim to ensure that all activities in the software life-cycle will, in time, be machine mediated and supported. This will provide four main benefits :

(1) **KBSA will be able to suggest plausible strategies for the design of any program modification, implement these via coding, and test the results.**

(2) With requirements and specifications captured in a machine readable and manipulatible form, **the specification itself becomes an executable prototype.** Thus specifications themselves can be validated.

(3) **Software implementation can be automated.** Whenever specifications are altered, the previous software development process which is resident in the KBSA, can be replayed with the new or modified specifications, and generate the new software. Thus rather than software patching, whole new and integrated code will be generated.

(4) The software development processes are all resident in the KSBA machine and hence **all the information necessary for software project management is recorded.** Consequently this can be massaged and manipulated, via inbuilt management routines, to **implement, and function as, a software project manager.**

It is noteworthy that ITD/ERL is currently negotiating with the USAF Rome Laboratory (ex-RADC) to have access to results to date, and participate in the development, of this product.

6.1.2.4 CUBE TOOL (TOU88)

CUBE TOOL, specifically developed for C^3I system development by Thomson-CSF of France, is a computer-based tool supporting the C^3I systems analysis, specifications of functional requirements, and C^3I systems design processes. It provides multi-views of requirements from the perspectives of the designer, the developer, and the end-user, and is used for coherency and consistency checks of data, processing and communications requirements.

It is more than just a software development support tool; rather it is a C^3I systems development tool.

Specifically CUBE TOOL :

(a) Records requirements and performs the specification of requirements and functional interdependencies, specifically for interconnected, geographically distributed C^3I system nodes.

(b) Captures and describes elementary automated and human-element C^3I processes and their related information exchanges, and hence their resultant communications requirements.
These are specified in a pseudo-code formalism (akin to Ada and Pascal, from which the former is derived) and a grammar which, with multi-windowing techniques, permit an analyst to deduce and analyse information flows, information transformations and exchanges of multi-media information (data, narrative (text and voice), video and imagery, and graphical user-machine interface formats) in normal C^3I operating and fallback modes, when different system nodes degrade or fail.

(c) Permits the calculation by summation, from the above, of the information flow, the information processing and communications requirements at any node, for different levels of operational conditions, thereby permitting the capability, type, and number of workstations, staffing, data-base management requirements and communications requirements to be specified and thereby leading to initial and indicative C^3I system requirements.

CUBE TOOL has been in development since 1981-83 and has now progressed to a reasonably user-friendly tool. It has been used to support the development of the NATO Air Command and Control System (ACCS).

6.1.2.5 The Technique of Exploratory Prototyping

Exploratory prototyping is a software-based method or technique for promoting dialogue between end-users and developers, and acts as a focus, for quickly exploring and eliciting user requirements, during the stages when the user has difficulties in articulating these. This has been treated previously in Section 5.4.1 above.

6.1.2.6 C^3I Software Development Process

The integration of C^3I software development tools with EA to provide a C^3I-specific proven software development process is still in its early days. However some successes has been claimed and demonstrated **(CUL88, GIO91).**

One such documented case example is the rapid and evolutionary development of the US Army Europe Tactical Command and Control System (UTACCS) **(GIO91)**, the co-developers being US Army CECOM and TRW as prime contractors. The strategy followed was that essentially described under EA in Section 5 and shown in Figure 4. A major new operational release, with improved capabilities, has been delivered every six months, with the corresponding development cycle for each release being eighteen months.

Of particular interest is the software development process used. The key to this is the choice of the software architecture, which is a loosely coupled, 4-layered architecture (see Section 8.3 and Figure 6). Each layer provides a specific set of services and interfaces which isolate the implementation details of the lower layers. The layering approach promotes significant software re-use and commercial-off-the-shelf (COTS) products.

The four layers are, beginning from the top layer :

(1) **Layer 1-Applications :** This layer implements the C^3I-mission unique capabilities. It forms the basis of user-oriented functions and is thus the layer on which the introduction of most new functional capabilities is focussed.Typical applications include : specific data-base applications; situation assessments based on maps and graphics; decision support aids; message applications; and so on.

(2) **Layer 2-UTACCS Support Software :** This layer implements service-oriented functions that directly support the applications layer, such as : user-machine interfaces; data distribution; information handling; information evaluation; (local) network control and monitoring; and so on. It also provides an application transparent interface to the lower-level COTS software such as the Operating System and communication services.

(3) **Layer 3-System Support Software :** This layer provides COTS system support such as a UNIX-based operating system, a relational data-base management system and various communications functions.

(4) **Layer 4-Hardware :** This is the hardware layer, partitioned into user services, and system services hardware.

Each system release cycle either adds products to each layer (primarily to the Applications layer and its supporting Layer 2), or replaces existing products with improved or expanded versions. Typically each release may have between 5 and 10 new, or improvements to existing, products.

The software development cycle for each system release begins with system developers nominating and allocating a set of products for that release, according to the long-term Evolutionary C^3I Development and Implementation Plan (ie roughly a C^3I System Migration Plan, see Section 9.2), itself based on the operations concept for the subject C^3I system. An analysis is carried out to assess the implementation requirements and any constraints to such. Considerations may include: the degree of user interaction; effect on system performance; complexity; partitioning of functions between multiple development teams (generally different teams allocated to different software layers); and so on. An **implementation plan** for each product is formulated, which may involve user interviews, prototyping, simulation, analytic modelling etc, or a specific combination of these, which, for given types of products, have been found to be optimum.

Thus for specific database applications, which is the most common improvement product, user requirements definition through interviews and operational prototyping have been found to be most effective. Functional requirements are largely dependent on data elements, on relationships, on types of transactions and reports, required by users. System engineers colocated at the C^3I site perform detailed requirements elicitation and development with the users, to define specific data elements, report formats, query formats etc, as well as **validation criteria.** The system engineers produce a "user requirements document" which the users review, validate and need to approve. Developers further develop this into a "thin specification" which contains a logical design and schema, screen and report layouts etc. Generally the next step is an "operational prototype" for demonstration to the user and user evaluation sessions. Depending on the complexity of the end-product, these prototypes may just be simply screen mock-ups showing layouts etc; or they may be animated sequences, based on "canned" or training scenarios, with user interaction and validation sessions. These are readily recognised as "exploratory prototypes" (section 5.4.1). For demonstrations and validation of a number of products, more elaborate prototypes approaching the "experimental prototypes" (section 5.4.2) are developed, with users validating the products under conditions approaching an operational environment. The code developed for, and used in, the latter prototypes, when validation is completed, becomes the end product.

Database applications software development also impacts on Layer 2 through the user-machine and data distribution interfaces. A common set of functions ("client library") defines the data distribution system interface.The aforementioned prototypes include procedures that interface the particular "client library".

The software end product is then formally released for Integration and Testing as the next step. This is done on a **testbed** which has simulations of the input/output of the operating system, and is configured as a a multi local area network, interconnected by packet switches (in this particular case) to represent the C^3I intercommunicating network in its current (and hence baseline) configuration, to test, verify and validate product integration into the C^3I system. Any problems are identified, documented and given priority for immediate correction by the software development team (or, if serious enough, the problem product is deferred from inclusion in the scheduled operational release).

A successful product then is released and integrated in the operational system for further detailed evaluation to include the viewpoint of the users. Functional and performance data are collected, assessed and, if necessary, ordered by priority action for future product releases.

The software process for changes to Layer 3 software products differs slightly in the early phases. Layer 3 products do not have direct user-machine interface components; hence user validation through any of the various prototypes is not required, nor is an "user requirements document". However after the software product is developed, testing and integration, including on the testbed, follows as for the previously described Applications layer products.

6.1.2.7 Open Systems and Commercial-Off-the-Shelf Software

C^3I must leverage on and take advantage of both the rapid developments in the commercial sector in Information Technology and Telecommunications and the dramatic drop in computer hardware systems and software costs.

Rapid developments can make for rapid obsolescence. Consequently C^3I systems based on proprietary software architectures and single vendor systems must be avoided. Proprietary systems have a history of being leap-frogged by newer developments They are expensive to support, the more so over an anticipated C^3I whole-life of 15-20 years. And vendors have little incentive, once they have won a long-term contract, to retain their best system and software designers on that contract; rather they put them on the development of new products.

The potential offered by the large number of developers and vendors of heterogeneous systems and platforms, applications and system support software in the commercial marketplace can only be realised if such multi-vendor, heterogeneous platforms and software can be interconnected and interworked in a sensibly transparent fashion. This will be the case if candidate platforms, workstations, systems etc, are compliant with **Open System Interconnection (OSI) standards,** a set of (now) emerging international standards, which enable interoperability between multi-vendor heterogeneous computers and connectivity through commercial local, national and international data communications networks **(ABR89, WEI83)**.

OSI standards are based on a 7-layer model formulated and approved by the International Standards Organization (ISO) (and hence the "ISO OSI 7-Layer Reference Model"), which breaks down the process of data transmission by a sender host computer to an addressee host computer, into a sequence of seven sub-processes; this results in modularity and eases the development and production of standards. "Lower layer" functions deal with physical communications, and links; the "higher layers" deal with functionality and applications. To communicate, both computers exchange approved protocols at each layer/subprocess, before proceeding to the next, higher layer (see Figure 6(a)).

The OSI reference model is only a framework for defining standards, and thus a wide variety of implementations in the computer hardware and software is permitted (ie OSI states "what has to be done", not "how it is to be done").

Several standards may be associated with each layer, and a sequence of OSI standards spanning the 7 layers, will differ from other sequences of OSI standards, depending on the particular application. For example data communications, e-mail and the transfer of files, will all have different OSI standards sequences. Such a sequence of standards is called an OSI Profile ie an "OSIP".

To ensure orderly development and growth of computer-based Information Systems, as well as to prevent "vendor lock-in", governments in Western Europe, North America, Japan, and recently Australia, have promulgated **GOSIPs** (Government OSI Profile), which vary according to particular functional requirements of the Information Systems they apply to, and with which commercial contracts must comply.

A C^3I-appropriate GOSIP needs be developed and which, in the first instance, enables a number of neccssary C^3I system functions (for example: communicate data; e-mail; transmit special format files; access and query special data-bases etc).

It is in the nature of Standards that as they evolve they subsume the previous standards so that compliance with the earlier standard is still retained, but greater capability made possible with the newer standard. The philosophy behind, and the nature of, the 7-layer model makes it possible, that over time, additional layers may be introduced, particularly at the higher applications-associated levels, to enhance capabilities (to assure C^3I system security, for example) (see Section 7.2). It must also be noted that proprietary vendor products which have "value-added", provided they are OSI (or appropriate GOSIP) compliant, should not be precluded from consideration for C^3I applications.

A step beyond OSI and the current ability for multi-vendor, heterogeneous computers to only intercommunicate, is **Open Systems,** a vision where users are not restricted by technical barriers, imposed by proprietary constraints, from taking advantage of multi-vendor platforms, multi-vendor system software, and multi-vendor applications software. A useful, working definition of Open Systems, by the CEO of Hewlett-Packard is **(DEP91)** :

> ..."an Open System is a set of networked heterogeneous computers that can work together as if they were a single integrated whole - no matter where the systems are located, no matter how they express their information, no matter what supplier produced them, and no matter what operating system they use"...

Open Systems should exhibit at least the four following qualities **(DEP91):**

(1) **Compatibility :** Applications running on a given existing system must be able to run future (software) releases.

(2) **Interoperability** : Systems must be able to interoperate, and interwork, on shared data.

(3) **Portability** : Applications running on a given hardware platform must be able to run on any vendor's platform of the same or similar class.

(4) **Scalability** : Applications should run on a full range of architectures from laptops to mainframes.

To implement Open Systems, the same set of published International Standards for software interfaces must be used. A start has been made to standardize operating systems (O/S), with the **UNIX** O/S, or refinements thereof, becoming the standard. UNIX is a multi-user, multi-tasking operating system which currently runs on a wide variety of platforms from micro- to mainframe computers. A further development is **POSIX** (Portable Operating System Interface for UniX), an

IEEE standard that defines the language interface between applications programs and the UNIX O/S; adherence to POSIX by UNIX vendors will ensure compatibility when programs are moved from one UNIX platform to other UNIX platforms. It needs be said, however, that despite the agreement to base operating system standards on UNIX, the industry is split into two competing UNIX camps, one centered around the "Open Systems Foundation", backed by IBM inter alia, the other around "UNIX International", backed by AT&T, where UNIX was originally developed; each is pushing for adoption of its own version of UNIX (of which there are many).

Other system support software to be considered is **X-Windows,** which is becoming a de-facto industry standard, for the design and implementation of user-machine graphics interfaces; and the Open System Foundations **OSF/Motif** which is a more general user-interface, is UNIX-compatible, and is being currently proposed as the user interface standard.

The "down side" of Open Systems, articulated by its critics (often from the big computer vendors) needs mention. Firstly, it is claimed, Open Systems "stifle" innovation once the standards are set. Secondly, the natural gravitation will be towards the "lowest common denominator". Consequently, the argument goes, products will be so generic that their users will sacrifice and miss out on the value-added features that proprietary products can offer. The simple counter argument is that compliance with Open Standards does not preclude value-added products, and the choice will be between lowest-common denominator and value-added Open Systems compliant products.

In parallel, **Commercial-off-the-shelf (COTS)** software, developed for the commercial, business and mass market, will be available for, and applicable to, C^3I in particular for CSS applications. Many software applications, which support information systems and management, including financial decision and planning support aids, for large commercial enterprises, are being developed, marketed and refined. These applications have their clear counterparts in C^3I. For example in information processing, the commercial software for e-mail has its C^3I counterpart in message transmission and processing. Commercial menu-driven word/text processing can be readily adapted for C^3I preparation of reports, plans, and orders.

Data base management systems have their obvious counterparts. In the decision and planning support and aids, commercial relational data-base applications have their military counterparts in correlation of narrative reports to the battlefield situation perception; graphic overlays for battlefield situation presentations; histogram, chart, 3-d views for military resource and logistics applications; and so on.

As the similarity between the operations of large commercial enterprises, aided by modern computer-based management and information systems, and that of Defence operations aided by C^3I systems becomes increasingly recognised, the range, and applicability of, COTS software products and applications to C^3I will greatly increase. However some problems with integration and compatability are likely and will need to be overcome.

6.1.2.8 C^3I System Security

An explicit requirement is that C^3I systems, by their mission, must be comprehensively secure, not susceptible to, and invulnerable from, any "information warfare" attack, and that the implementation of security measures to ensure these must hamper neither functionality nor interoperability.

Any **security architecture** (which can be defined as .."an environment consisting of a set of logical components and operational protocols needed to provide security to, and protection of, C^3I system entities and resources"..) must address global C^3I information security and hence : software security; (individual) computer security; network security; communications/data and information distribution security; personnel security; and physical security. The objective must be to provide a **"Trusted C^3I System Base"**, analogous to a "trusted computer system".

In particular, security need be implemented in an OSI environment, with data, information and intelligence being transmitted via commercial sector communications and distribution networks, and with an increasing proportion of systems and applications software being COTS and Open Systems compliant.

Another key requirement is that the resultant security architecture, must result in a **multi-level security (MLS) environment,** as there will be multiple users, cleared to different levels of security, and handling and processing information itself at different levels of security. An MLS environment permits such operation without compromising security.

Typical security services which will be mandated include :

(a) **Information Integrity** : protection against unauthorised modification, loss, or repetition of user information.

(b) **User Information Security** : protection of user information from disclosure by unauthorised sources.

(c) **Access Control** : protection against unauthorised access to user/C^{3}I resources from a far/remote user.

(d) **Traffic Security** : protection of information related to source, destination and transport of information within the C^{3}I system or with other lateral and Allied C^{3}I systems.

(e) **User Authentication** : verification of the identity of a remote user.

With the proposed implementation of ADF C^{3}I systems in an OSI, COTS environment, the starting point for any proposed C^{3}I Security Architecture should be based on the ISO OSI 7-layer model, and on the placement of security protocols and functions within one, several or all the layers of the OSI model. To that end, ISO, and some NATO Working Groups, have been attempting to define standards for a Security Architecture for the OSI model **(BAR87).** Some other initial analyses **(COH87)** suggest placement of security functions at Layers 3, 4 and 7 to achieve MLS. Other approaches, in particular based on commercially available Trusted Computing Base elements, also show promise.

7 C^3I Subsystems and Supporting Technologies

7.1. Surveillance and Information Collection System (SICS)

7.1.1 Structure and Functions of the SICS

7.1.1.1 Roles and Functions

The Surveillance and Information Collection System (SICS) is to consist of the facilities, staff and procedures which together effect surveillance on, and sense over, the region of interest, and collect, in a timely fashion and in sufficient detail and accuracy, data and information on the current state, disposition and location of potential and existing enemies and on the surrounding environment (terrain, weather, etc). Its role is to collect data and information to be passed on to the Intelligence and Information System (IOFIS) for further processing, massaging, fusing, aggregating etc to produce intelligence which, on subsequent assessment and evaluation, provides "indication and warning" on the nature, capability, location and intent of existing or potential enemy entities.

7.1.1.2 Structure

The SICS will consist of a number of surveillance assets and sensors which are either organic to the assets under the control of a commander, or may be assigned to him by a higher HQ for the duration of his mission. The commander, through the SICS, will have access also to the products of other national and allied surveillance and information collection systems. The commander will task the SICS as required to seek surveillance information on specific targets and areas of interest; he may also seek and request similar information from other national and Allied SICSs.

In general, the surveillance sensors and assets constituting a SICS would have been acquired and justified on single-Service and other considerations outside the framework of C^3I. In the future this may not be the case.

Associated with the sensors and information collection facilities are operators, procedures, various SICS processing capabilities, and voice and data communications to distribute the SICS data and products and to accept tasking.

SICS products vary over a wide range, and depend on sensor classes, types, sensor platforms, missions, number of sensors, sensor revisit times, associated processing etc. Thus the product may vary from "existence of an unknown target" to full identification and location (class; type; identity; location; speed, direction and, if appropriate, height).

Surveillance sensors depend on **class** (whether **active**, such as radar; or **semi-active**, with a passive sensor and an active source illuminating the target, such as the sun, for **photo-reconnaissance and infrared (IR) detection**; or **passive**, with sensors responding to target own radiation, as in **IR sensors**, or to target signal emissions, as in **signal intercept sensors**); on **type** (whether **radar**, or **IR**, or **electro-optic**, or **acoustic**, or **E S M intercept**); on **mission** (**wide-area surveillance**; or **sector surveillance**; or to support **point-defence** etc.); on **platform** (**space-based**; or **ground-based**; or **airborne** (manned or unmanned); or **sea-surface**; or **sub-surface**; **mobile**; or **fixed**); as well as on **surveillance report and information formats** (whether **voice** or **narrative/text reports**; **radar blips** or **tracks**; recorded **signal intercepts**; or **imagery**; or **photography**; etc); on **data update rates** depending on platform motion, search and scan patterns; and generally on the implementation of a "surveillance collection plan", whether ad hoc or formally structured.

The wide diversity of both surveillance sensors and information collection assets must be noted. It is this very diversity that will provide a good deal of the robustness in the SICS, in particular when the C^3I, system is under stress, such as in times of tension and hostilities. It can be argued that to consider a SICS architecture, in the sense of some a priori well planned and specified architecture would work against this robustness. In any case SICS assets are in place, having grown and been acquired over time outside the context of an integrated C^3I, concept; most of SICS assets are not integral with or organic to C^3I but are under the operational control of individual uniformed Services or other Defence agencies.

7.1.1.3 SICS Products

Each SICS product ("SICS report") needs to be tagged with its source sensor, position of sensor at time of report, time of sensing, as well as with a measure or level of confidence attributed to the report, which would be based on the type and degree of local processing of the surveillance/sensor data at the SICS site; for example if any aggregation or fusing of data from two or more sensors of the same or different class, type etc to reconcile ambiguities and reduce uncertainty were used or, to provide better target recognition, classification and identification, by means of comparing sensor outputs with stored data characterizing known targets.

In the case of ADF C^3I, surveillance assets and sensors constituting a SICS would range, inter alia, from: surveillance on an opportunity basis by voice reports from observers, such as civil aircraft pilots, coastwatchers, etc; to tactical surveillance products from P-3C maritime patrol aircraft from radar, ESM and other on-board sensors; to battlefield surveillance such as pilot/aircrew, Forward Artillery Observers etc by voice, and from possibly UAVs; to strategic surveillance such as from the JORN OTH radars; to surveillance products from allied systems such as the US Ocean Surveillance Information System (OSIS) Baseline Upgrade (OBU) System at the Maritime Command Centre (see Section 7.2.2.4.b); and to allied surveillance satellites currently, and in the future, to a possibly national reconnaissance satellite.

7.1.2 R&D Activities in Support of the SICS

1. **A comprehensive census of existing, planned and (likely) future ADF surveillance, sensor and information collection assets needs be made** to enable their integration into an unified C^3I, system and in particular:

(a) to determine the baseline SICS capabilities and to identify any limitations to, or gaps in, capabilities;

(b) to provide a key input into any National Surveillance and Information Collection Plan, which is required to ensure that optimal use of SICS assets is made at any point in time to provide the information, and eventual intelligence, to meet existing national and Defence objectives;

(c) to identify the nature and structure, and quantify as required, the SICS data and information flows, both within itself, and to other C^3I (sub)systems, in particular to the Intelligence and Information System (IOFIS); to assure that communications channel bandwidth and capacity is not exceeded in times of C^3I system stress and has sufficient allowance for future growth; and that IOFIS data communications and information processing requirements are commensurate with the SICS output products interfacing with the IOFIS.

This needs to include the nature of the SICS data, information, reports, products etc; their media (voice; text/narrative; imagery;etc); statistics on their size, frequency of generation, peak values of these etc; their level of security; as well as the associated quality and reliability, in the clear, and under EW/Information Warfare conditions; by sensor type, locality, level of conflict intensity etc.

The degree of post-processing associated with each sensor etc, and the degree and type of collation, aggregation, fusion etc, if any, at SICS nodes or prior to transmission to the IOFIS need also be obtained.

(d) to characterize, quantify and assess the response times of tasking individual SICS elements, so as to determine their adequacy or otherwise for C^3I purposes during different levels of stress and usage.

2. **Investigate and implement a "SICS Resources" Data-base** to be available to authorised C^3I system users, which in conjunction with a AI-based **SICS Management System,** will enable them to plan and optimally use and task SICS elements for specific surveillance and information collection in support of the C&C function; and investigate methods of integrating both of these into the C^3I system.

3. **Investigate data and information fusion implementations and applications** appropriate to be carried out at SICS elements and nodes, and prior to transmission to the IOFIS.

7.1.3 Technologies, Tools and Methods Suppporting the SICS

Tools to construct a "SICS Resources" database are available. Several "sensor management" applications based on Expert-systems have been reported in the literature (see in particular (WAL90)).

7.2 The Intelligence and Own-Forces Information System (IOFIS)

7.2.1 Structure and Functions of the IOFIS

7.2.1.1. Roles and Functions

The Intelligence and Own-Forces Information System (IOFIS) needs to consist of the facilities, staff and procedures which together provide the means to receive, store, maintain, collate, evaluate, analyse, integrate (or "fuse") and interpret information collected and obtained from the SICS, to create intelligence on the past, current, and likely state, disposition, location, and intent of existing or potential threats, and distribute this in a timely manner, in a selection of standard, easily understood and assimilatable formats to the commander, his staff, and other authorised users.

In addition, it also needs to provide the means to maintain, update and collate, and integrate with the above intelligence picture as required, the operational and administration information available, or reported from own (and allied) forces, on the state, readiness, state of supply, disposition and location of own forces and assets and those of allies and other friendly troops; as well as have the means, tools and facilities to access and interoperate with other information systems (such as geographical information systems (GIS), national, State, and public sector data bases etc) as are required to support operations and administration of the ADF.

7.2.1.2. Structure

It follows from the above that the IOFIS should consist of two distinct subsystems:

(a) The **Intelligence Subsystem (INTS),** being the means and assets which, from SICS and other inputs, generate intelligence on enemy or potential enemy entities ie on essentially non-cooperative entities, in the region of interest.

(b) The **Own-Forces Information Subsystem (OFINFS),** being the means and assets which maintain, collate, and update operational and administration information on own, allied and friendly forces ie on cooperative entities.

This division is made not only because the two subsystems produce different products, but also because they use different means and methods of collection and reports as their inputs, and have been, by organization and tradition, separate.

7.2.1.3 Intelligence Subsystem (INTS)

The INTS has as inputs reports from the SICS and its sensors, reports from allied and other cooperating agencies, as well as reports from own forces in contact with or observing the non-cooperating entities. Inputs are as a consequence of an associated "Intelligence Collection Plan" (which could be a subset of, or a particular instance of, a National Surveillance and Information Collection Plan (see Section 7.1.2.1)) to meet the particular intelligence requirements of a Commander.

> **Intelligence Collection Plan:** A plan for gathering information from all available sources to meet an intelligence requirement. Specifically, a logical plan for transforming the essential elements of information into orders or requests to sources, within a required time limit. **(JSP84).**

The process by which information thus obtained is converted into intelligence and transmitted to the Commander (and other authorised users) follows the accepted **"intelligence cycle" (JSP84)**, which consists of four basic sequential subprocesses, with each of which therefore a corresponding (sub)system may be associated with.

(a) **Planning and Direction Subsystem**
This identifies the absence of, and hence the requirement for, specific intelligence; prepares a "collection plan" (with the support of appropriate decision and planning aids and in concert with the SICS Management System (section 7.1.2.2)); issues orders and requests to the SICS and other collection assets and agencies; and monitors the performance and checks on the productivity of the tasked collection systems, assets and agencies (ie essentially performs the command and control function for intelligence collection).

(b) **Collection Subsystem**
This receives the information from the SICS and other sources via the Communication System on behalf of the INTS, and routes it to the appropriate elements of the (subsequent) Processing Subsystem; and generally provides the information management functions of the raw, unprocessed incoming information (logging; labelling; time, source tagging etc).

(c) **Processing Subsystem**
This converts the information into intelligence through analysis, comparison, integration/ ggregation/ fusion, evaluation and interpretation by human and computer-aided elements, and prepaies the resulting intelligence products into easily understood and assimilatible formats for distribution.

(d) **Dissemination Subsystem**
This makes available, in a timely fashion, or transmits as required, to the commander, and other authorised users, the intelligence in an appropriate and easily assimilatible form via the C^{3}I Communications System, or as required, by other means.

Supporting the above are other facilities, including :

(a) the **Intelligence Data Base,** which is the sum of intelligence data, information, knowledge, and finished intelligence products available to, and supporting the C^{3}I system, and comprising of a number of specialised and structured databases, with their associated database management systems, including a geographic database on the region of interest, and in particular,

(b) a **Geographical Information System (GIS),** which may be defined as :

> ....an organised collection of computer hardware, software, geographic data, and personnel designed to efficiently capture, store, update, manipulate, analyse and display all forms of geographically referenced information..(quoted in **(WIL91)**).

Since reliable, comprehensive and detailed intelligence on the environment of an area of operations is vital for the success of operations, it therefore is a key requirement for the ADF. Thus :

> ....the availability of comprehensive and up-to-date military maps and charts, together with a detailed knowledge of the environment and its infrastructure, is fundamental to the effective control of military operations.... **(DOA87)**

The successful implementation of a GIS would go a long way to satisfying this requirement.

The roles for the GIS are both for strategic intelligence, and tactical intelligence and operations planning and support. **"Strategic"** would include the development and maintenance of the GIS, development and update of the GIS databases, in particular the collection of comprehensive terrain data (including physiographic, hydrographic, vegetation, environmental/climatic, cultural (specifically features and objects which impact on military operations), and oceanographic) for Australia's region of interest, as well as the development of generic applications; GIS applications would, inter alia, establish patterns, discern trends and changes to established patterns, and aid in visual modelling (eg provide answers to "what if ?"questions as an aid to determine intent). For **tactical applications,** subsets of the GIS would form part of the Command Support System (section 7.3) and GIS databases for specific areas of operations would be available to the Commander and his staff for intelligence and planning of operations; for example to determine line-of-sight coverage from designated observation points (or have the optimum observation point determined subject to specified constraints); indicate areas of concealment; likely rapidity of movement for dismounted ground-troops; mobility of wheeled and tracked vehicles, on road or off-road; suitability of sites for helicopter, light aircraft etc landings; communications coverage at different RF bands due to topography, propagation conditions etc; acoustic subsurface propagations and consequent coverage areas; air defence SAM coverage zones as function of aircraft height and and other factors; etc. Additionally, spatial/map displays can be augmented by multi-media, such as colour imagery of user-selected terrain, cultural features etc, tabulated data, narrative text and so on, to provide comprehensive computer aids to planning and decisions

Useful references on GIS are **(BUR90, WIL91)**.

7.2.1.4 Own-Forces Information Subsystem (OF-INFS)

The OF-INFS will have as inputs reports on operational and administration matters from own forces and from national and Allied cooperating agencies. Current reporting is generally by means of dedicated and specific communications and by other agreed procedures, which are, in the main and for historical reasons, single-Service based. In accord with the concept of joint, rather than single-Service, operations, the role of HQADF, and consistent with C^3I being about the management of own Defence resources, a set of new reporting procedures need be developed and implemented under an "Own-Forces Information Collection Plan", analogous to a Intelligence Collection Plan.

> **Own-Forces Information Collection Plan**: A plan for the organised reporting by, and collection from, own forces of operational and administration information on their state, readiness, state of supply, disposition and location, as well as from cooperating national and Allied agencies and other entities such as mapping agencies, PTTs (Postal, Telegraph and Telephone (Authorities)), domestic and civil airline authorities, domestic and civil shipping authorities etc, for other information relevant to ADF operations and administration. The Plan needs to specify the information required, formats to be used, means and frequency of reporting, and timescales to be met.**(Proposed Definition).**

The process by which this information is received, assimilated, processed and transmitted to authorised users would, by analogy with the "Intelligence Cycle", follow an **"Own-Forces Information Cycle"**, with analogous subsystems and facilities (preceding section), and need not be repeated here.

7.2.1.5 IOFIS Network

Both of the above systems, INTS and OF-INFS, are specific examples of the broader class of distributed "information systems", and are probably akin to "Office Systems", due to the existence within each of workgroups ("subsystems") each carrying out specific computer-aided activities.

> **Office System :** A set of application programs specific to the workgroup to which they are applied, able to exchange information whether text, data or image, with other relevant applications within the context of a hardware platform, conforming to the standards adopted by the organisation (from (**BES91**)).

For successful implementation, Office Systems, being particular instances of Information Systems, need to to be related to the specific business objectives of the organisation, but the facilities provided need to automate, or provide computer-mediation of, particular processes common to one or more group of workers (**BES91**). Clearly the workgroups and the corresponding Office Systems will be linked by Local Area Networks (LAN), with the enterprise/organisation linked by a much larger LAN; and which, due to the nature of the information being managed and processed, would to some degree ease the implementation of Multi-level Security.

Information Engineering methods (Section 6.1.2.2) need to be applied to determine the specific objectives, group structure, information flows, and decision criteria of each workgroup.as well as of the overall organisation, for the successful implementation of the IOFIS.

7.2.2 Issues Relating to the IOFIS

7.2.2.1 IOFIS Databases

The processes in the INTS and OF-INFS are data and knowledge intensive. The associated large amounts of data and knowledge have long persistence and need be accessed by multiple and often concurrently running applications. Both data and applications are often complex, with complex relationships, and increasingly multi-media, image and graphically and spatially oriented. The IOFIS architecture will need to reflect this and thus needs to be structured around a number of specialised databases.

The increasing complexity of the data being processed and manipulated makes conventional and current databases and their associated database management systems (DBMS) inadequate (**JOS91**).

First-generation DBMS, based on either hierarchical or network data organisation, require frequent data reorganisation as new data types are added; as well they exhibit a natural upper limit to their size.

Second-generation, relational DBs, and associated relational DBMSs, have a tabular data structure based on rows and columns, which caters well for simple data types such as numbers and strings of text, and is more than adequate for commercial, well defined applications (for which it was developed), with well-structured data, and handling short duration transactions. This data organisation does not lend itself readily to handle complex data, which often may be incomplete, has complex inter-relationships, is used increasingly for graphic and spatial applications, and may be involved in long transactions of several hours or even days. Applications utilising these types of complex data are increasingly using object-oriented languages and paradigms optimised 'o manipulate these complex entities as "objects" (Section 6.1.2.1). The resulting mismatch (the so called "impedance mismatch" problem) between data representation in the database and that required in the applications program may require 30% or more additional application code to perform the required data translation (**JOS91**).

Consequently, **third-generation databases based on object-oriented data structures** (ie stored data no longer containing records (of n-tuples) but instead "objects") **called orientated databases (OODB)** are in development and in early product release. A good comprehensive overview of OODB's is (**JOS91**).

The principal advantages of OODB's include **(JOS91)** :

(1) "rich" data modelling (ie data, generally complex, that is defined by the user in a natural way), which is compatible with, and encouraged by, object-oriented (O-O) methods and in particular, O-O programming languages;

(2) the elimination of "impedance mismatches" (resulting in unobtrusive or "seamless" interaction between databases and applications);

(3) sharing of objects among applications written in different languages (since object implementation is hidden by the O-O paradigm, the particular language used is not relevant);

(4) distributed, platform independent object storage, important for multimedia applications, with large volumes of information, worked on and shared between separate users, possibly using heterogeneous computer platforms;

(5) retention of the ability to access database objects both by query, and by navigation;

(6) transactions for concurrent and groupwork, such as in "office system" environments, and where the duration of transactions can be counted in hours or days, are well supported **(ATW91)**.

Two approaches to OODB implementation are being pursued **(JOS91)**:

(a) an **evolutionary strategy,** articulated in the "Third Generation Database Manifesto", advocates **the extension of relational databases with objects.** This approach is advantageous when an evolutionary migration from existing, in-place relational databases to OODBs is important;

(b) a **revolutionary strategy**, articulated by the "Object Oriented Database Manifesto", advocates **a total ground-up approach of developing a total object-oriented database technology**. This approach is advantageous when integration of databases with existing object-oriented software, and any potential impedance mismatches and associated software development overheads are important issues.

An example of an implemented OODB, for a prototype (French) Navy Command and Control System, using multi-media displays is described in **(BAR89)**.

7.2.2.2 Multi-media, Hypertext and Hypermedia

The term "multi-media" has been used in this Report to mean data, information and knowledge in a wide range of forms and media, including voice, numerical, text (free-form and formatted), graphics, imagery and video.

Hypertext (meaning "beyond" or "extended" text) **is non-sequential presentation of text or information.** It is generally accepted to mean the process of generating and accessing text and graphics in a non-linear or non-sequential way by enabling the "reader" or user to choose his own sequence of accessing the information by invoking his own choices from those presented to him (by the hypertext document author). In current usage, Hypertext refer to computer-based tools and methods to generate and use hypertext.

A Hypertext document ("hyperdocument") is structured and organised (by its author) so that its information is cross-connected by "links" and "nodes". A "link" is always displayed to the user and is most often in the form of an index, giving options to the user to select his next choice in his personal sequence of accessing the information in the document. His link selection routes him to a "node" which can be a (new, explanatory) paragraph, a new file, another document, a figure, photograph etc. From there, the available links can either reroute him back to where he had been, or he can "navigate" to new parts of the document **(SWI91)**. This process of "reading" a document and absorbing the knowledge therein is common enough in the "hard-copy" world; examples include (as in this Report) : "see Figure x", "refer to Section y", "for more information, consult z".

Hypermedia is Hypertext augmented by audio, animated graphics and video. Both of these terms thus relate to the non-sequential manipulation and accessing of multi-media data, information and knowledge.

Hypertext/hypermedia provides powerful computer tools for :

(1) structuring knowledge representation and creating knowledge bases;

(2) creating structures of information and knowledge, organised to meet specific user requirements (including structures patterned to meet individual user requirements) which via links and nodes matched to specific knowledge applications, enable endusers to "navigate" through anticipated pathways to access and transfer knowledge in natural user language and in easily assimilatable forms;

(3) creating an environment for **work group collaboration** in the above **(SWI91).**

Hypertext/Hypermedia thus promises to provide the tools for the creation and manipulation of "living" documents, in a work group environment.

The Hypertext process seems very applicable to the process of creating, through analysis, collation and "fusion" of multi-source multi-media information, knowledge bases as well as the hyperdocuments themselves supporting intelligence assessments, situation assessments etc worked on and prepared by group efforts, and which can be structured in formats for specific applications, such as to support a commander in his CSS. Similarly, other "living"documents, such as strategic and tactical military plans developed in peacetime (perhaps including the C^3I Master plan itself?) can be constructed as hyperdocuments, and be amended and evolve to meet changing situations and circumstances.

The high potential for Hypertext/Hypermedia to implement effectively computer-aided creation of Intelligence (hyper)documents in the IOFIS to support the broad C^3I mission in general, and that of the Command and control mission in particular, requires serious investigation. This should include both the preparation, through group work, of comprehensive intelligence products in easily manipulatible and assimilatable forms, and their end use, as hyperdocuments inherently lend themselves to user customisation for the optimum transfer of knowledge contained therein, for particular applications. A comprehensive reference, including a description and assessment of currently available Hypertext/Hypermedia tools, is **(FRA89).**

Finally, the vision for Hypertext/hypermedia is for universal utilisation, by the "literate" rather than just by the "computer literate", as well as for the elimination of what are seen as constraints on this imposed by the prevailing incompatibility between various multi-vendor computers, operating systems, data bases, Public LANs etc. **(FRA89).** The Hypermedia "culture" thus sees as its objectives not only computer-based information and knowledge presentation and its transfer to be natural, effective and user-centered (as well as universally implemented), but also to achieve user-friendliness to the extent of minimising, even eliminating, the need for computer literacy, and for total Open Standards in computing. On any of these bases alone, Hypertext/Hypermedia warrants serious attention.

7.2.2.3.Other Issues

Any proposed architecture, design and implementation of the IOFIS need to be based on defined information requirements and information flows which properly reflect system functionalities; otherwise the resulting system does not add value to the existing (IOFIS) processes, rather it leads to user dissatisfaction at increased operational costs. The two issues here are:

(a) the maturity, and application, of Information Engineering methods to define the system called the IOFIS; and, in particular,

(b) the nature of the "intelligence culture", which Information Engineering methods are required to "intrude" on in order to describe its operations and processes.

a. The "Intelligence Culture"

The intent here is to flag the issue rather than propose any solutions.

The Intelligence community on which the IOFIS would impact on is secretive by nature for several (good) reasons. Tradition aside, these include : the nature of the information elements of this community handle; the products they produce; the processes they use to convert the former into the latter; and the nature of the links they have with overseas/Allied like communities. Consequently they guard their workings and assets jealously; are seen by others as parsimonious in the sharing ot their products; and often report directly to their political masters. Until recently (in Australia), they had no direct oversight by the military, or intimate links with the ADF, for C^3I directly, or with other potential IOFIS stakeholders.

Cognisance of the sensitivities of the Intelligence community must be exhibited by other IOFIS and C^3I stakeholders.

b. Information Engineering and IOFIS

Information Engineering methods, applied to produce effective Information Systems within any given organisation, require consistent views of the mission and strategic objectives of that organisation, its organisational structure, and information types, structure, and flows; the resultant information is then integrated and will be reflected in any proposed IOFIS system architecture.

In the situation when different groups and organisations become part of the IOFIS process, as well as other and different organisations being authorised to request IOFIS end products, the likelihood of each having different perceptions about the mission and objectives of the IOFIS - in particular that of the Intelligence community with the above mentioned "cultural" mindset - is very high. The danger exists that any resultant IOFIS, rather than being effective, let alone efficient, could consist of "islands of automation", unable - or unwilling - to communicate with each other.

The issue then is similar to that which Evolutionary Development and Acquisition has to overcome, although on a different plane: namely that understanding, and agreement, of the functionality, and of the underlying processes, of the IOFIS, will take some time to elicit, as conflicting viewpoints are gradually resolved and converge.

c. Standards and OODBs (JOS91)

In the two main strategies to implement OODBs, there is a large diversity of approaches. The development and acceptance of standards for OODBs would greatly accelerate their production and implementation.

Recently the American National Standards Institute (ANSI) has established a Task Group to examine this issue. Their methodology is familiar : define a common "reference model" for OODBs based on O-O methods for both the applications programming and the Data Management System; assess and identify where in the OODB processes standards are possible and useful; and recommend, approve, and disseminate the resultant standards. Separately, a US industry consortium (the "Object Management Group"), has been formed to examine the standards issue from an O-O applications integration framework, to accelerate the development of O-O complementary technologies to improve the portability of O-O based applications.

Both standardisation efforts are based on the principles of "layering" (section 8.3).

7.2.2.4 IOFIS Ongoing Efforts

a. ADFDIS

The Defence Intelligence Organisation (DIO) has as some of the key objectives of its Corporate Plan the development of plans to enhance secure systems for the collection, receipt, storage, display, retrieval and distribution or archiving of information both within DIO, as well as to and from DIO customers; and to establish and maintain an associated secure communications network to enable the above.

The ADF Distributed Information System (ADFDIS) is being proposed to meet those ends. Specifically it is to be a system of Intelligence databases shared between DIO, Joint Commands, subordinate formations and other specified Units to support ADF Intelligence requirements. Technical control and management of ADFDIS will be centralised under DIO; but certain Joint and Environmental Command-specific functions will be devolved down to the corresponding Commands. By both its function and its users, ADFDIS will require both distributed database and multi-level security architectures.

b. MCAUST OBU

MCAust have installed as its Maritime Command Support System, a US delivered subsystem designed to both receive the "ocean surveillance products" (OSP) disseminated in real-time by the US Navy's OBU system (OSIS (Ocean Surveillance Information System) Baseline Upgrade), as well as accept as inputs the RAN's own maritime surveillance reports.

OSIS **(GRA82)** is :

> ...a network of personnel, facilities, computers, communications and procedures designed to receive, process, correlate and disseminate evaluated ocean surveillance information.. (It) provides near real-time, all-source indication and warning, threat assessment, positional and movement information, and over-the-horizon targeting (OTH-T) support to (US) national, theatre and fleet users..

OSIS consists of two main subsystems :

(1) "Sea Watch" which provides ocean surveillance information to high-level (US) users in the Washington D.C. area, and

(2) OBS (OSIS Baseline System), which supports USN fleets and other selected users including MCAust.

It is OBS which is the heart of the system; it receives information from a variety of sensors (including those of allies), which is then automatically processed, correlated, evaluated and disseminated as OSPs in a variety of formats to authorised users in near real-time through secure communications. **The current version (OBU) processes information on own and foreign naval, military and air forces.** Users employ the received information (OSPs) to assist in making decisions on the deployment and utilisation of (maritime) forces.

OBS consists of three main subsystems :

(a) **Communications Processing Subsystem** which receives incoming reports and disseminates OSPs; performs data formatting; performs incoming message error detection and correction; logs message traffic; and performs subsystem control.

(b) **Analysis Processing Subsystem** which provides various analysis aids, including trend analysis; performs automatic and computer-assisted manual correlation of reports; provides automatic alerts of "significant events"; provides message generation and retrieval; generates track data base updates; and provides various databases and graphics support.

(c) **Word Processing Subsystem** which provides an efficient message creation and editing capability; text insertion into intelligence messages; computer-aided message composition; and selection of formats for dissemination of OSPs.

The current version, OBU (ie the OSIS Baseline Upgrade) has improvements to the real-time throughput, the number and type of targets handled, database enhancements, and operation workstation enhancements, including interactivity **(GRA82).**

From the above it is clear that **OBU could form a very useful baseline system to study as a model for the IOFIS, both for the INTS and the INFS.** Its roles and functions (with the exclusion of its supporting surveillance sensors which are not organicaliy part of it) meet most of those expected of a C^3I system, for both peacetime and in the event of hostilities. It is worthwhile quoting at some length from **(GRA82)** :

> **In peacetime**, ocean surveillance is used primarily in the development of estimates of capabilities and intentions and for indications and warning. The (OBU) gives a commander the ability to focus on developing crisis areas and high-interest targets, and it permits the general surveillance of large ocean areas.
>
> ...**In wartime** the (OBU) provides the flexibility for forces to be selectively and rapidly concentrated in widely separated ocean areas...It supports the commander by providing him near real-time identification and accurate positional data with high confidence and timeliness... **It provides the commander with the vital information necessary for maximum effective use of forces..** (emphases added).

7.2.3 R&D Activities in Support of the IOFIS

1. In collaboration with the various IOFIS stakeholders, and in particularly with DIO, suitable **Information Engineering methods and tools need be investigated as the first necessary step to define the agreed objectives and functionalities of the proposed** IOFIS; the processes within the IOFIS need to be defined and quantified; and the incoming, internal and outgoing data and information structures and flows need to be identified and characterised.

2. With agreement from, and in collaboration with, MCAUST, **the system architecture of, and the processes within, the OBU should be investigated and evaluated with the objectives of assessing its suitability as a basic model for the IOFIS system architecture,** as well as to determine its eventual integration with and migration into the longer term ADF C^3I systems.

3. By agreement with, and through sponsorship by, DIO, and using agreed Information Engineering methods, **the system architectures of both ADFDIS and the C^3I system proposed herein need be aligned and made consistent; an agreed early implementation of ADFDIS needs be defined and characterised as a Baseline IOFIS system; and in collaboration with IOFIS stakeholders, an IOFIS Migration Plan** to transition the Baseline ADFDIS to an envisioned IOFIS system of a national C^3I system **needs be developed.**

4. The **ongoing DSTO R&D on Geographical Information Systems (GIS) needs be coordinated**, as well as coordinated with ongoing work in other areas of the ADF (in particular with the Army's Directorate of Survey) and Defence, as well as with civil/public sector authorities (Land and Survey Departments etc), particularly in the areas of standards and capture and transmission of data. **GIS COTS tools and products developed in the commercial sector need be monitored, evaluated and, if appropriate, implemented whenever possible.**

The **work on terrain intelligence in ITD/ERL (MOR91) needs be better sponsored and supported,** in particular with the objective of supporting multi-media terrain intelligence bases in Australia's region of interest.

5. **Third-generation or Object-oriented Databases (OODB), in particular OODBs based on extending second-generation relational databases (RDB) to store and manipulate objects, need be investigated and evaluated, as well as methods for migrating RDBs to OODBs.** Commercial developments and standardisation efforts in this area need be monitored.

6.**The integration of databases storing information in different media, in particular spatial information and images, and their cooperative working to support multi-media applications, needs to be investigated**

7.The **technologies for multi-media information processing, including optical compact-disk (CD) technology**, for read-only memory (ROM) applications and also with Read/Write capabilities, for high-density storage multi-media databases, **need be monitored and products evaluated.**

8. **Hypertext/Hypermedia tools and methods need be investigated, evaluated and** tailored for IOFIS processes and applications.

9. A **multi-level security architecture (MLS) for the IOFIS**, consistent with the needs and sensitivities of the Intelligence Community as well as consistent with any global security architecture implemented in future ADF C^3I systems, **needs be developed and implemented.**

10. **Developments in the commercial sector in the rapidly expanding field of Information Systems and allied areas, together with their supporting tools and methods**, in particular Information Engineering and those concerned with "strategic business information systems", **need be monitored, wherever pos^ible products evaluated, and if applicable and suitable, applied.**

7.2.4 Technologies, Tools and Methods Suppporting the IOFIS

The development- and product-rich environments of Information Technology, Information Systems, Information Engineering etc, and their allied technologies, in particular dominated by the commercial sector, has many tools, methods and processes which can support the development and implementation of the IOFIS. They are too numerous to mention; some have already been mentioned in passing, or discussed in some detail in the preceding Sections.

7.3 The Command Support System (CSS)

7.3.1 Structure and Functions of the CSS

7.3.1.1. Roles and Functions

The Command Support System (CSS) is to consist of facilities, staff and procedures which provide the means for the Commander to carry out his command and control role effectively in accomplishing his mission in general, and some objective in particular.(Author's Note : CSS is not to be confused with the "Combat Services Support", also "CSS", a subsystem of AUSTACCS (see Section 7.3.1.5.b(iii))).

Specifically the CSS provides the means to the Commander and his staff of accessing, in a timely manner, intelligence and information from the IOFIS, in a suitable and easily assimilatable form, together with facilities, including automated and computer-aided, for : situation picture generation; situation assessment; generation and presentation of possible courses of action; analysis and selection of a preferred course of action; supporting mission planning and associated logistics plans in support of the preferred course of action; generation of plans, orders and tasking; transmission and communications of plans, orders and tasking to appropriate units for execution; monitoring the progress of missions and evaluating and, as necessary, controlling them; communicating with superior, lateral and subordinate and, if applicable, with Allied, commanders; and communicating, as necessary, with other C^3I subsytems.

7.3.1.2 Command and Control Processes

A CSS has always existed in the ADF and its individual Services, and exists now, although in its current form it is very distributed, very manually intensive and at present with basic computer aids only.

The requirement for a modern computer-based CSS is part of the much broader C^3I response to the increased demands on the Commander and his staff brought on by technology. These technology developments have resulted in a vast expansion in the space and volume requiring surveillance, and likewise in the size of the potential area of operations. Simultaneously the time available to react has decreased, due to the ever increasing range, speed and accuracy of weapons, together with current mobility and deployment capabilities of forces. However with the use of tools and aids offered through Information Technology and Telecommunications, the commander and his staff now have the potential capability of receiving intelligence and information, assessing the resulting situation facing them, making quality decisions, plan and carry out operations, all quicker than the enemy can, thereby enabling him to operate within the enemy's decision cycle. A computer-based CSS gives a Commander the ability to proact rather than react and to dictate to the enemy by creating considered and well-planned events.

The proposed computer-based CSS will need to reflect in the first instance the traditional commander's staff structure organised around Staff functions (and hence around the key command and control associated subprocesses) of Personnel, Intelligence, Operations and Plans, Logistics etc (in US usage, corresponding roughly to the G-1, G-2, G-3, and G-4 sections respectively). ADF Joint Force HQ are somewhat differently organised, being divided into two main functional areas, an Operations Branch (consisting of the functional areas of Plans, Operations, Intelligence and Communications) and an Administrative Branch (consisting of the functional areas of Personnel, Logistics and Specialist Advisers (Medical, Chaplain, Provost Marshal etc)). The exact mix and strength of each Branch depends on the particular mission at hand. The proposed CSS therefore needs to be reconfigurable both by size and along functionality.

These functional areas naturally reflect the processes associated with command and control, and thus provide a basis for aggregating them into groups of associated sub-processes which in turn can sensibly be considered candidate CSS subsystems to which automation and other particular computer aids and tools can be applied.

The following is one such suggested sequence of grouped subprocesses, (six in all, from (a) to (f)), which together may be said to comprise one cycle of the command and control process; it is based broadly on Figure 2 (in particular those parts within the "Command HQ" block), the ADF Joint Force HQ Staff structure, and in part on **(SOC87, KIN88)** :

(a) **Intelligence Subprocess** includes :

* **Situation Monitoring** (based on downloading geographical data from an IOFIS-based GIS appropriate for the area of operations, on downloaded situation pictures from the IOFIS/INTS for the corresponding area, and likewise on downloaded historical, doctrinal technical and biographical data pertaining to the enemy; monitoring updated enemy situation reports, ORBATs etc in the area of operations; merging and

correlating reports from troops and assets under own control; merging and correlating weather and localised terrain reports; etc).

* **Own forces and resources status monitoring** (based on information downloaded from the IOFIS/INFS and updated by own forces reports; Rules of Engagement; monitoring of status, readiness, location etc of own C^3I (sub)system; etc).

* **Evaluation of the relative status of own and opposing forces and assets.**

* **Situation Assessment** (general enemy capabilities downloaded from IOFIS/INTS; inference of the likely impact of the environment on the situation; prediction of enemy capabilities, intent and likely behaviour in area of operation;).

(b) **Options and Planning Subprocess** includes :

* **"What if" and "Why not" analyses of Situation Assessment** with due regard for Commander's given missions and objectives.

* **Generation of Options/Courses of Actions**, including "Maintaining Status" (ie continue with intelligence gathering and situation monitoring).

* **Preparation and "gross-detail" planning for each option ; evaluation of each plan** (for feasibility, consistency, completeness, achievability and likelihood of success).

* **Detailed planning of selected Option/Course of Action** (including allocation of resources, Logistics Plan and other supporting planning).

(c) **Decision Subprocess** (the **"Command"** Function) includes :

* **Evaluation of Courses of Action** and their supporting "gross-detail" plans.

* **Selection of a preferred Course of Action**, including requests from higher echelon HQ.

* **Assignment of resources** (Units, weapons, other assets, commanders etc) for execution of the selected Course of Action.

* **Issuing of Orders** to execute the selected Course of Action.

* **Modification**, or as as necessary, the rescinding **of outstanding orders.**

(d) **Operations Preparations, Scheduling and Control Subprocess** includes :

* **Refinement of plans and schedules** as required.

* **Assigning missions, objectives, tasks and duties** to individual units and assets.

* **Generation of orders, task and duties instructions** to execute the selected Course of Action.

* **Operations Execution/Force Employment monitoring** (the **"Control"** Function) (determination of the success or failure of own forces; fine-tuning of plans and objectives as required; evaluation of battle damage; assessing the need for additional forces and assets; assessing the need for surveillance, reconnaissance and information collection).

(e) **Communications Subprocess** includes :

- **Preparation and formatting of orders, tasking and allocated duties for transmission** to recipients.

- **Dissemination of new, modified or rescinded orders, tasking,** etc.

- **Receiving of reports, orders etc** (including from surveillance sensors and assets organic to a commander's force, and reports from own forces).

- **Interfacing with C^{3}I Communications System and report on its status** (current configuration; reconfiguration; communications EW activity; CS survivability; etc).

- **Monitoring, administering and generally managing CSS communications.**

(f) **General Administration Subprocesses** include :

- **Administering and assigning tasking as required to specialist staff** (Medical, Chaplains, Provost marshal etc).

- **Management and control of the CSS and of the C^{3}I system as a whole.**

- **Applications and general software support for CSS computer facilities.**

- **Other management and duties** not falling within the ambit of the above subprocesses.

7.3.1.3 CSS Requirements

To perform the above command and control process effectively and efficiently, the following are required :

(a) rapid and timely access to IOFIS databases;

(b) availability of knowledge bases appropriate to the mission, threat, area of operations etc, to support decision aids for situation assessments, Courses of Action, mission planning aids, etc;

(c) information to be presented in clear, readily assimilatable formats selectable according to the preferences of the commander and his staff;

(d) applications programs for each of the above functional areas, including CSS-local supporting databases downloaded from the IOFIS, appropriate to mission- , threat- and area of operations-specific information and knowledge;

(e) the capability of extendability as new CSS applications are developed;

(f) computer tools to generate plans and orders in the necessary formats;

(g) a base set of plans for the specific missions and objectives consistent with the areas of operations, in formats which may be readily amended, updated and fine-tuned to match developing scenarios, as well as contingencies;

(h) a capability to exchange information between CSS user workstations, with extendability to support "groupware" (computer-based tools and applications which support and augment group-work eg preparation of plans);

(i) a C^3I system management and control capability, including a means of displaying the status, availability, location, current tasking etc, of the C^3I system as a whole, as well as user-selected views of individual C^3I subsystems;

(j) a communications capability for both CSS-internal communications and external communications.

In addition :

(k) an inbuilt capability to reconfigure, and as necessary, expand rapidly to meet contingencies, as well as the capability to permit "customisation" to reflect a Commander's personal style of command and control;

(l) commonality and replicability with other CSSs at different echelons, and lateral CSSs.

7.3.1.4 Structure

The CSS will need to consist of a number of Military Information (sub)Systems, each associated with one of the six subprocesses described in some detail above in Section 7.3.1.2, structured in groups of workstations accessing databases and running applications associated with the corresponding sub-processes.

The above CSS subprocesses comprehensively describe the command and control process. However practical CSS functions, structures, layouts etc need be user-requirements related and dependent. Consequently any detailed CSS structure at this stage is premature. A CSS structured around the following subsystems is proposed as a candidate CSS :

(a) a CSS Intelligence Subsystem;

(b) a CSS Planning and Options Subsystem;

(c) a CSS Decision Subsystem;

(d) a CSS Operations Control Subsystem;

(e) a Communications Subsystem;

(f) a CSS Management Subsystem;

with each supported by domain specific databases and applications, and communicating with and having access to their corresponding counterparts in the overall C^3I system, and in particular with the IOFIS.

7.3.1.5 CSS Ongoing Efforts

a. JP 2030

The major ongoing CSS development for the ADF is JP 2030, the HQADF CSS. The objective is to have a core system installed by the end of 1993.

Requirements, inter alia, include : the incorporation of Intelligence and spatial/geographical information databases to support command and control; interactive graphics capabilities; computer-aided preparation and interpretation of formatted messages; appropriate communications interfaces to support information exchange; and an appropriate software development environment (**AND89**).

Some preliminary work on user requirements had been conducted by ITD/ERL, primarily to determine and define the recently formed HQADF organisational structure and the information exchange transactions therein **(DEE90)**, a manually intensive and restricted form of Information Engineering.

JP 2030 has recently undergone some major project management reorganisation and more detailed "elicitation of user requirements" will be undertaken and planned to be completed by the end of 1991; development, including prototyping, is scheduled for 1992. Evolutionary Acquisition has been recommended by ITD/ERL **(HEN91)**.

b. Other ADF Projects

A number of other and single-Service systems, to support command and administrative functions are in various stages of current or near-term development. They can be described as having limited capability, based primarily on formal message exchange, with limited graphical support (with the exception of AUSTACCS, see below), and have been designed to conform with pre-existing, manually intensive procedures. **(AND89)** briefly describes them (with some emphasis on their communications requirements). They include:

(i) Navy

(a) **Navy 1226 : Maritime CSS.** This is based on the US Navy's OBU and is essentially an IOFIS rather than a CSS; it is described in Section 7.2.2.4.b.

(b) **Navy 1286 : Maritime Command Centre Communication and Information Distribution System.** By its name it complements the OBU so that together they form a Maritime CSS.

(c) **Navy 1609 : Maritime Intelligence Support Terminal (MIST)**, for shipboard use.

(ii) Air Force

(a) **BACSS** (Basic Air Command Support System). An initial, minimum system, to provide a secure and independent communications (ie not using existing or proposed Defence communications) and information storage system.

(b) **ASMA** (RAF Air Staff Management Aid). A RAF single-vendor-platform-based electronic bulletin board for disseminating "volatile", date-time stamped operational and resource status information in specific formats and governed by Standard Operating Procedures. It is a computer-based system linking ACAUST with eleven fixed and two deployable RAAF sites.

It currently is used as an interim BACSS.

(c) **ACAUST CSS.** A longer term project to meet the Air Environmental CSS.

(iii) Army

(a) **AUSTACCS** (Australian Army Tactical Automated Command and Control System). Currently in procurement, this is a tactical battlefield system which receives, processes, retrieves existing, and disseminates battlefield information, to other more specialised battlefield systems and higher HQs. It is essentially a message-based system but will also have extensive tactical computer-generated battle-maps based on digital terrain models. Although AUSTACCS has been identified as a tactical system, it is proposed to be deployed in LCAUST HQ.

(b) **COMPOPS** (Army Operations Room Computerised Operations System). A computer-based system to support Intelligence, operations and plans via formatted messages and applications (to be developed). An "interim" system, it is expected to support the definition of requirements for the Army's portion of JP 2030.

(c) **Strategic Plan 2005**. The Army's master plan to integrate all of the above, as well as interface and interoperate with other single-Service and HQADF CSSs.

(iv) Defence

These are mainly Administrative support systems, and include :

(a) **MSRP** (Manpower System Redevelopment Project).A distributed computer-based personnel records and pay system.

(b) **SSRP** (Supply Systems Redevelopment Project). A computer-based system to support the supply and logistics system.

(c) **FSRP** (Financial Systems Redevelopment Project). A computer-based system for financial resource management.

The above list is very possibly dated and may not include more recent projects and proposals.

c. Overseas CSS Developments

Overseas CSS projects and developments have occasionally been referred to in this report.

(a) **NATO** as part of its C^{3}I system is developing a CSS based on a modular structure **(SOCH87, SCH89).**

(b) **UTACCS** (US Army Europe Tactical Command and Control System) **(GIO91)** is briefly described in Section 6.1.2.6 from its system software architecture perspective.

(c) **AC2SMAN** (Alaskan Command and Control System Military Automated Network) **(HOO91)** is a PC-based system providing commanders in the Alaskan Theatre of Operations information on the location, composition, and readiness status of own and enemy forces in an interactive and highly assimilatable form. An opportunity exists for collaboration with the USAF in this area.

The development of the **US Navy's CCC (CInC Command Center) and TCC (Tactical Command Center) under the proposed "Copernicus" Architecture,** the USN'S vision for C^{4}I (C^{3}I with Computers) **(COP91)** need be monitored.

In addition there are a number of (mainly single-Service) US developments specific to the CSS proposed subsystems listed in Section 7.3.1.4 above. These include :

(a) The USAF's **APS (Advanced Planning System) (UNI91)**, a AI/Expert System-based set of decision and planning aids to support USAF's Tactical Air Force missions and combat operations, being co-developed by UNISYS, and based on a number of prototype decision aid and mission planning tools, including :

(1) **TEMPLAR** (Tactical Expert Mission Planner);

(2) **TDA** (Tactical Decision Aid);

(3) **FLAPS** (Force Level Automated Mission Planner);

(4) **C3CM BMDA** (C^3 Counter Measures Battle Management Decision Aid).

(b) The US Army's **ALBM ATTD** (Air-Land Battle Management Advanced Technology Transition Demonstration) **(USA90)** is somewhat analogous to the APS. It is an Expert System-based and knowledge-based set of tools to automate support for the production of a faster planning cycle specifically in the areas of coordinated staff planning, developing options and multiple Courses of Action, assessing these, developing tactical plans, automating the development and production of plans, automating the monitoring and comparison of battle execution etc. For each of these subprocesses specific expert system-based applications (called "advisors") are being developed (eg. "enemy situation threat advisor"; for the battlefield area, a "terrain advisor"; for the friendly situation, a "capability advisor" etc) .

(c) The USN under its "Copernicus" C^4I Architecture vision will be developing analogous tools to these as well.

7.3.2 R&D Activities in Support of the CSS

1. **Tools, methods and techniques to support the elicitation of CSS user requirements need to be evaluated and as necessary further developed, in particular the technique of rapid prototyping** through story-boarding, and using COTS tools wherever applicable.

2. **The command and control process**, together with the supporting subprocesses as described in Section 7.3.1.2 above, **need to be better defined** in collaboration with, and agreement of, the ADF end-users.

3. **The functional, structural and physical layout architectures of the CSS need definition**, in particular the scheme of partitioning the command and control process into the several subsystems suggested in Section 7.3.2.3, the number of workstations for each subsystem, the requirements for structured cabling etc for fixed and mobile CSS sites, and with CSS reconfigurability and extendability in mind.

4. **The nature and scope of the command and control support aids need be investigated, scoped and tailored to meet particular ADF CSS needs,** including decision aids for assessing the enemy threat situations, the friendly situation, the battlefield terrain and environment situation, Course of Action aids, mission planning aids, computer-aided plan generators, in collaboration with ADF experts in these separate domains. The nature of decision aids in the presence of large uncertainty and in particular in the presence of deception needs particular attention. **This may involve collaborative R&D activities through existing, or by initiating new, cooperative agreements with Allies.**

5. Because the CSS, and in particular the man-machine workstation interfaces, are the means by which the commander and his staff interface and interact with the C^3I system, **investigations into timely and optimum information presentation is required, in particular regarding the optimum transfer and assimilatability of the information and knowledge presented. This needs to include hypertext/hypermedia and its supporting technologies** for the integration of multi-source, multi-media data and information such as images, high quality spatial/geographical information, video and weather, bathemetry (for some situations) and, increasingly in the future, satellite coverage and footprints.

6. Associated with this, **investigations are needed into man-machine interfaces, from the viewpoint of user-friendliness, optimum information presentation and transfer**, and wherever appropriate, COTS and conforming with Open Standards. The Human Factors issues of such investigations should include :

(a) Size and placement of screens, menus, windows etc;

(b) Display management : keyboards, trackballs,touchscreens, icons etc;

(c) Visuals of overlays, symbology, colour, deconfliction between these, visual clutter etc.

7. **The requirements and specifications of CSS workstations supporting CSS applications in multi-media need be developed**, and need be based on the technical requirements related to anticipated information processing, information throughputs, and consequent communications requirements for each group of functional subsystems, their internetworking architecture, and with reconfigurability and extendability of the CSS in mind to meet various contingencies; as well as being compliant with Open Standards wherever possible.

8. As the modern command and control process, by its nature, is team oriented in its specific functional areas and requires decisions to be made at the end of each subprocess, **computer-assisted and mediated group work ("groupware"), as well as the nature of, and any computer aids for, group decision making** (including decision making under stress), **need be investigated.**

9. To carry out effectively many of the above investigations and evaluate realistically the performance of various CSS proposals and their attendant tradeoffs, **a comprehensive and versatile CSS testbed needs to be funded and developed, complemented by a realistic scenario generator** (see Section 5.5 on the LCSS).

10. Realistic CSS investigations and performance evaluation require the following supporting investigations and activities :

(a) **the collection of field data and other empirical data and information relating to command and control, and the setting up of an associated database;**

(b) the transformation of this data to support **realistic and real-time Command and Control scenario generation;**

(c) **appropriate mathematical models and simulation facilities;**

(d) **the development of Command and Control metrics, measures of performance, measures of effectiveness** etc to assess the performance of the CSS and that of individual subsystems.

7.3.3 Technologies, Tools and Methods Suppporting the CSS

Relevant tools, methods and techniques have been referred to throughout this section. These include rapid prototyping via story-boarding; appropriate hardware and software simulation tools for the proposed CSS testbed; and a number of expert-system based tools for decision aids and mission planning. Many of these are common to the development of the IOFIS, and have been mentioned in that context.

R&D activity in this area is intense in overseas Defence R&D laboratories. Access to these CSS enabling technologies and specific tools need be pursued through existing bilateral or multilateral collaborative agreements, and new agreements should , if necessary, be initiated.

7.4 The Communications System (CS)

7.4.1 Structure and Functions of the CS

7.4.1.1 Roles and Functions

The Communications System (CS) is to consist of facilities, staff and procedures which together provide the means :

(a) to enable the Commander to communicate with his superiors and with his assigned forces on the "Command Net";

(b) to enable communications between C^3I (sub)systems and elements for tasking, requests, reports and so on, including communications relating to personnel management, logistics, specific battlefield functional communications etc;

(c) to distribute data, information and, as requested, intelligence between C^3I (sub)systems and authorised users;

(d) to enable communications between lateral and, as necessary, allied C^3I systems;

(e) to interface with existing Defence, and single-Service, dedicated communications networks.

It is heartening to note that the recent "Defence Communications Corporate Plan 1991-2001" (DCC91) has recognised the real role of military communications namely (and quoting directly) :

> **...The Defence Communications Mission (is) to provide communications for the command and control of the ADF and the management of the Defence organisation...**

7.4.1.2 Limitations of Current Defence and C^3I Communications

Current Defence communications and infrastructure are inadequate to meet the communications requirements of ADF C^3I for a number historical, systems-oriented and technical reasons (AND89) :

(a) Existing and near-term/planned ADF communications are the result of single-Service requirements, reflecting command and control processes practised to date and the carrying out of operations (and hence interoperability) with the corresponding Service of Allies, rather than, as now required, as part of joint ADF forces in joint (ADF) operations, and under joint command. The result is that currently communications are Service-specific "islands of communications and networks", with limited connectivity, rather inflexible, and with better interoperability with Allies(!) than with other elements of the ADF.

(b) Many of the recently installed or near-term strategic (long-haul) communications systems, such as DISCON (which replaces the in-place DEFCOMMNET) and the associated DPSDN (Defence Packet Switched Data Network), as well as single-Service tactical systems, have, in the main, been replacements for existing systems, with all their attendant limitations. Interconnectivity, and hence interoperability, is very limited, and enabled at only several entry points; this is mainly limited to HF, and hence capable of supporting low data rates only.

Many of these systems eg DISCON, and the Army's tactical trunk communications system, PARAKEET, are "orphan"systems, in that their architectures and coding, signal and multiplexing formats do not conform to existing civil sector standards, precluding their ability to interface either with existing, or with proposed and soon-to-be installed, civil communication networks, such as ISDN (Integrated Services Digital Network), other than by purpose-developed, and hence expensive, gateways.

(c) The transmission bandwidth of the great majority of the existing and near-term systems is, by anticipated C^3I requirements, very low and inadequate.

DEFCOMMNET supports, for most links, a 1200 bits/s voice channel at HF, divided into sixteen 75 bits/s secure telegraph (telex) channels.

DISCON, essentially Defence's private network, has a basic channel capacity of 32 kbits/s, which can be multiplexed up to 2 Mbits/s for data transmission. Secure (digital) voice is at the basic 32 kbits/s, while secure facsimile can be at 2.4, 16, or 32 kbits/s. Telex message traffic can be either at 300 or 2400 bits/s. DISCON will eventually consist of three overlaid networks operating in three different transmission media: a terrestrial line-of-sight network, principally provided by Telecom through their 2 Mbits/s digital bearer; a (future) HF network of limited connectivity, for telegraph signalling at 300 and 2400 bits/s for emergency C^3I functions; and a Satcom capability, via the proposed DEFAUSSAT, with some eleven fixed stations, and two mobile ones, with a planned bandwidth of up to 54 Mhz. Discon uses leased Telecom and Aussat services; but owns exchanges and Satcom ground stations.

Single-Service systems, such as the Army's PARAKEET, have 16 kbits/s channels which can be aggregated, via time-division-multiplexing, to provide 512 kbits/s data transmission, and in some cases doubled again.Through special gateways at specific network nodes, it can interface with: Combat Net Radio; DISCON at both HF and at wideband 256 kbits/s; and Telecom and OTC. Its narrow band HF links can support three-four 3 Khz channels at 2400 bits/s for telegraph, data, and digital voice. Extensive use of Aussat to provide a mobile, secure, high capacity capability is planned.

Naval and Air Force communications, due to their long-haul nature, have to date been at HF, primarily at 2400 bits/s. Air Force also use UHF for tactical C^3I (air-to-air and air-ground-air command and coordination); Navy use some UHF for inter-ship communications as well.

Greater, and system-specific, detail of existing and near-term ADF communications may be found in **(AND89).**

The trend in C^3I now, in particular in data, information, and intelligence is increasingly towards multi-media (voice, formatted/narrative text, facsimile, graphics, maps, imagery, video etc), and in digital form almost exclusively. Bandwidths requirements to accommodate data transmission rates of 10-100's Mbits/s will be required. This is clearly in excess of current or near-term Defence communications capabilities.

7.4.2 Required C^3I Communications Capability : ISDN and B-ISDN.

Due to the limited connectivity, interoperability and relative inflexibility of current ADF communications assets, together with the anticipated growth in usage and requirement for multi-media, wide-bandwidth C^3I communications, it is concluded that a new C^3I communications capability is required. Such a capability is too costly to be implemented by a wholly-owned ADF or Defence communications network. Rather such a network should:

(a) increasingly be based on architectures and national and international standards compatible with current world-wide developments in the civil/commercial telecommunications area **(AND89);**

(b) increasingly be leveraged on such developments;

(c) exploit and utilise as much as practicably possible the new telecommunications infrastructure and assets associated with these developments being put into place in Australia by Telecom (and, in the near future, by some other commercial entity as well).

In particular, these civil sector developments are the **Integrated Services Digital Network** (ISDN), currently being implemented world-wide and in Australia as well, and its follow-on system, **Broadband-ISDN (B-ISDN).**

The process by which ISDN is being evolved and implemented will make the resulting telecommunications network robust and "future proof". The widespread use of the civil/public sector communications infrastructure for Defence communications in general, and for C^3I in particular, not only would result in large scale cost savings (equipment economies of scale and existing infrastructure cost sharing) but, through the "seamless" interfaces and access to the extensive civil network and the resulting routing redundency, would enhance the survivability of Defence and C^3I communications **(AND89).** Finally, as the US DOD, NATO (and within it, the UK) and France, are, for similar reasons, migrating to ISDN and later to B-ISDN for their C^3I communications requirements

(GAG87, COV88, WID88, LEG89, VHO89, WEL89), the problem of interoperability of the ADF with Allies will thereby be greatly eased, while at the same time ensuring interoperability between individual ADF elements.

The increasing use of the civil sector infrastructure for Defence communications (and hence for the ADF's C^3I communications) has been accepted by Defence and this policy has been announced **(FSR91)**. These are further detailed in the Defence Communications Corporate Plan **(DCC91)**, in particular :

(a) .."The services provided by the national civil communications infrastructure are extensive and continued development of their capabilities is planned during this decade. Efficient use of national resources suggests maximum practicable use by Defence, particularly when competition is likely to lead to more extensive and efficient civil services"...

(b) .."Use the civil infrastructure to the maximum extent possible for maintenance of communications without incurring a loss in operational capability"....

7.4.2.1 ISDN and B-ISDN

ISDN is the projected world-wide public telecommunications network capable of supporting a number of digital communications transmission services including digital voice, digital data, e-mail, and limited-motion video-conferencing. The CCITT (French acronym for the "International Consultative Committee for Telegraphy and Telephony", the relevant committee of the International Telecommunication Union) definition of ISDN is:

> .. a network evolved from the telephony integrated digital network (IDN) that provides end-to-end digital connectivity to support a wide range of services, including voice and non-voice services, to which users have access by a limited set of standard multi-purpose *customer interfaces..*

The initial ISDN standards were defined only in 1984.

The key feature (and hence the key problem also) is the integration of the traditional voice telephony, with non-voice communications, initially data, facsimile, e-mail (and limited motion video-conferencing) and, in its follow-on system B-ISDN, with full video (broadcast and conferencing), imagery, and possibly High Definition TV (HDTV).

7.4.2.2 ISDN and C^3I

When fully implemented, ISDN will meet many of the requirements for C^3I communications, in particular its likely multi-media aspects. It is also worthwhile to quote the US DCA position on ISDN **(COV88)**:

> ...DoD (Department of Defense) requirements can be satisfied within an ISDN-based architecture; the ISDN is recognised throughout the world; and, **there is no competing future architecture inside or outside the DoD, other than those based on** ISDN...(own emphasis added).

The NATO C^3 communications subsystem is to be based on an NATO adapted ISDN reference architecture **(NISDN)** which can be defined as **(VHO89)**:

> ..a long range (twenty or more years), concept for changes and adaptations required in NATO's basic communications infrastructure. It leads to a universal NATO digital communications system based upon CCITT/ISO and commercial ISDN standards.
> ..It should use to the maximum extent possible national resources and accommodate as many communications resources built to different standards as is feasible...

7.4.2.3 ISDN Services

The CCITT recommended basic service for ISDN are two 64 Kbits/s channels ("B" channel) each for digital voice or data and one 16 Kbits/s channel ("D"channel) for signalling and low speed data, giving a total of 144 Kbits/s (the so called "2B+D" service); this requires the "basic access" interface. Through multiplexing up to 30 "B" channels and using an augmented "D" channel of 64 Kbits/s, data rates of 2 Mbits/s can be provided; these are primarily for Private Branch Exchanges (PBX) or Local Area Networks (LAN), and require the "primary rate access" interface.

ISDN will use a layered protocol model to define the interface protocols, corresponding to the ISO OSI 7-layer model.

The contrasting operational characteristics and constraints associated with each type of service (voice, data etc) resulting in differing delay sensitivities, different bandwidth requirements, possible congestion, bursty or continuous transmissions etc, have led to the recommendation for the switching and transmission mechanisms to be based on the "Asynchronous Transfer Mode" (ATM) (a packet-oriented transfer mode using asynchronous time-division multiplexing) and, consequently that any proposed Defence Communications Plan implementation needs to be based on ATM-based architectures as well **(AND89).** This ATM issue is by no means settled, in particular for the follow-on B-ISDN.The possibility exists that hybrids of both ATM and "synchronous transfer mode" (STM) may yet be required **(AAR91).**

7.4.2.4 ISDN and OSI

ISDN has its origins in telephony and initially concerns itself with (communications) transport technology. To meet its intended objective of "end-to-end" connectivity, it **must integrate seamlessly with existing systems compliant with the ISO OSI set of standards** (section 6.1.2.7) which are (and have been) developed and already implemented for data communications. An example of the successful integration of multi-vendor ISDN- and separate OSI-compliant systems has recently been reported in **(DII91).**

7.4.2.5 Other ISDN Network Issues

Local Area Networks (LAN) generally now consist of a range of OSI-compliant multi-vendor computer systems which are interconnected over distances of up to several kilometres (such as is likely in the IOFIS and CSS) through physically dedicated cables, the nature of which determines the maximum data transmission rate (thus, twisted pair cables support up to several mbits/s while fibre optic cables currently support up to 100-200 mbits/s rates). LANs in turn can either be internetworked with each other directly, or through a Public Data Network , via "gateways" (an interface or protocol conversion device). ISDN and in particular B-ISDN have the potential of replacing LANs by providing direct connectivity between computers through the ISDN network. However it is more likely that hybrids will result, with LANs retained to provide customised and value-added services which are not available in ISDN or B-ISDN **(LAT88).**

ISDN needs also to integrate with Satellite Communications ("SatCom") networks which have developed through their own evolutionary process. CCITT have been addressing this problem and have made progress to this end **(POT87).**

The problem of secure communications with ISDN and specifications and implementation of appropriate protocols has been considered by some; initial conclusions are that ISDN provides a practical infrastructure for secure communications throughout its network, in particular due to its end-to-end connectivity and the potential offered by the "D" signalling channel for key distribution and authentication **(STE88).**

7.4.2.6 "Militarising" ISDN

The genesis of ISDN, and its follow on B-ISDN, is in the civil telecommunications sector, and its intended use is in benign, non-hostile "civilian" environments. It therefore does not, in its present envisioned form, support certain specific military communications requirements (**MER86, WID88, LEG89, SCH89**). NATO has identified at least eight additional "special military features" required of ISDN (**SCH89**), which can be aggregated into four military requirements categories: **Survivability; Security; Interoperability**; and **Network/System Management and Control**. These are being addressed by NATO and include the provision of a lean and robust "emergency (communications) overlay" network accessible only to certain authorised C^3I users.

The process of formulating ISDN standards relating to broad and specific ISDN capabilities includes all three sectors of the telecommunications business: the various national (public and private) Postal Telegraph and Telephone administrations (the "PTT's"); the users; and the telecommunications products industries. These participate through open invitation to the CCITT technical committees to formulate and determine the relevant standards. If any sector, say the (military) user sector, wishes to influence particular existing, or introduce new, capabilities, then the possibility exists to have these considered by bringing them up via their national representative.

7.4.2.7 Shortcomings of ISDN

Some existing shortcomings of ISDN have already been alluded to (cf. for C^3I applications, the necessity to "militarise" it; the need to overcome the technical and network problems of integrating with existing communications systems which have evolved separately such as SatCom networks, and existing networks and products which are separately OSI-compliant and so on).

A serious criticism levelled at ISDN is the slowness of it being implemented and delivered to commercial users in general; and for Defence and C^3I users in particular, that the pace and timetable of installing ISDN-based communications is being determined by entities outside their control. (**RON90**) summarises some of the reasons for these delays. Some of these are due to the rearrangement of the ways business is being conducted by two (of the three) key sectors of the telecommunications industry, namely the PTT's (having to cope with the general worldwide trend of government deregulation and the opening up to competition, including in Australia), and the equipment manufacturers (having to cope with takeovers and mergers); and some of which ..

> ...can be traced to the timidity on the part of network operators, combined with the proliferation of (quasi-proprietary) "ISDN-like" services provided by other means...

Trial ISDN implementations with limited services offerings are in place in the UK, France, Japan, and to a lesser extent in the US. In Australia ISDN was launched in mid-1989 (**DOU89**). From the experience of these trial networks, refinement of CCITT standards, and the (almost) parallel development of B-ISDN, full service ISDN implementations should begin to proliferate from about 1992 onwards.

7.4.2.8 Broadband-ISDN

ISDN, from its beginning, was to allow, through evolution, a total integration of broadband services (**HAN89**), including:

(a) **bearer services** (communications facilities and transmission media, such as land-lines (in particular fibre optic lines), microwave relay, SatCom etc);

(b) **teleservices** (communications facilities enabling information to be transmitted from one point to some other specified addressee);

(c) **interactive services** (communications facilities enabling information exchange between two or more users based on alternating messages and replies);

(d) **distribution services** (communications facilities enabling information to be communicated to a number of authorised addressees);

for both business and residential premises.

The first ISDN standards were promulgated in 1984. CCITT began to work on B-ISDN in 1985. The first trial networks are expected in 1991-92; and the first commercial services may be offered by 1995.

B-ISDN is to have data transmission rates of two orders of magnitude or more than ISDN, ie in the range of 100-200 Mbits/s (140 Mbits/s is the expected minimum needed for HDTV). Based on fibre optic land lines, and with the above range of services, the goal transmission rates, and either ATM or hybrid ATM/STM switch implementation, B-ISDN will cater for the anticipated multi-media communications requirements for C^3I.

Telecom Australia has defined a six-phase development and implementation strategy for B-ISDN (**DAY90**). "Phase1 B-ISDN", based on ATM switches and primarily to support data communications between LANs, is to be introduced in 1995-6. "Phase 2 B-ISDN", extending to real-time services such as voice and video (of current broadcast TV quality) is to be introduced by 1997-8. A mature B-ISDN network supporting HDTV and economic video services is to be in place by the early part of the next decade.

7.4.2.9 The Defence Communications Corporate Plan 1991-2001

The Defence Communications Corporate Plan 1991-2001 (**DCC91**) identifies Defence communications objectives and gives indicative and very broad planning guidelines on how to achieve these objectives. It is intended to update the Plan at regular intervals.

The Plan recognises the mission of Defence communications as .."providing communications for command and control of the ADF and the management of the Defence organisation"..ie communications is there to support C^3I in the broadest sense as defined in Section 3.1 of this Report.

Further it is accepted in the Plan that military communications based on defence-specific (and hence "orphan") standards is not the way ahead; rather the way forward is to leverage on developments in the civil communications sector with their associated national and international standards. It is worthwhile to quote directly :

- .."Development of standards specifically for the defence environment will decline"....
- .."Compliance with international civil standards for communications is expected to become increasingly important. National standards will therefore follow agreed international standards"....
- .."Future military communications systems are expected to be based on civil digital standards as these are less expensive, more widely used and offer the advantage of easy interconnection with the vast civil network"....
- .."Adopt national digital communications standards. Where national standards are not available or allied interoperability precludes the use of national standards, adopt appropriate international civil or military communications standards"....
- .."Work more closely with civil communications authorities, industry, allies and with standards and regulatory authorities"....
- .."Migrate current systems, or elements thereof, to national digital standards when they fall due for replacement"....

7.4.3 R&D Activities in Support of the Communications System (CS)

1. Using (AND89) as a starting point, as well as (DCC91), **a comprehensive census of existing and near-term ADF communications systems, facilities and assets, needs be undertaken** by CD/ERL, in collaboration with HQADF and other elements of Defence and ADF as necessary, with the following objectives:

(a) determine the baseline CS capabilities, and identify any limitations to, or gaps in, capabilities required of the CS;

(b) assess the resultant baseline CS, as well as of dedicated single-Service communications systems, for compatibility and integration with ISDN and B-ISDN; and as necessary evaluate the technical feasibility, desirability, degree of integration, and cost-benefit of such of such integration.

(c) reconcile and integrate the results as much as is possible with the Defence Communications Corporate Plan (DCC91).

2. **The collation of data, information and communication flows** both within, and between, C^3I (sub)systems, as well as with lateral and allied C^3I systems, **is required to determine the overall C^3I system communications requirements.** In particular, for each system, facility, asset etc, the following, inter alia, are required:

(a) the nature of the communications (data; reports; information and intelligence products; etc);

(b) the corresponding mode or medium (voice; data; text/narrative; facsimile; imagery; real-time video; etc);

(c) the associated qualifying descriptors (level of security; level of priority; level of perishability; level of reliability; etc);

(d) the susceptibility and vulnerability to EW and Information Warfare attack.

3. **Measures of performance (MOP) and measures of effectiveness (MOE) for the CS need be developed** for typical C^3I scenarios and operating conditions, in collaboration and agreement with C^3I system stakeholders, in particular the end-users, **together with agreed methods of applying these.**

4. Consistent with the Defence Communications Corporate Plan, through early consultation and in collaboration with Telecom Australia, **methods and procedures need to be devised and implemented to ensure that the development of the ISDN and B-ISDN networks meets Defence and ADF communications needs in general, and of C^3I in particular,** with particular emphasis on the specific geographical locations of the various C^3I system elements. This should include participation in tests of trial Telecom ISDN and B-ISDN networks

5. A CS Migration Plan needs to be developed, consistent with the Defence Communications Strategic Plan.

6. Specific ADF "military" requirements, currently not encompassed within ISDN and B-ISDN, need be identified, investigated, and possible technical solutions developed (probably initially with advice from, and possibly in collaboration with, Allies, through existing, or as required new, collaborative agreements), but most likely co-developed and implemented in collaboration with Telecom (and any other future telecommunications operator in Australia).This includes CS network configuration management, network and network element monitoring, reconfiguring and rerouting as necessary etc , in particular when the CS network is under stress or suffers due to physical attack, together with investigations of the requirement for, and nature of, a robust, survivable, and necessarily lower-bandwidth back-up or "overlay" network to ensure survivability of critical C^{3}I communications.

7. **Methods and procedures to influence the development of ISDN and B-ISDN standards so that they incorporate ADF "military requirements" currently lacking, need be investigated, and developed,** in collaboration with Allies whenever possible, and certainly with Telecom, and implemented, **in particular by influencing the appropriate CCITT committees determining the relevant standards.**

8. **The feasibility of the early establishment of a basic long-haul ISDN-based CS testbed to gain familiarity with ISDN (and later B-ISDN) and to carry out CS-related investigations should be explored.** One end of the testbed should be in CD/ERL, the other at CSSG/ITD/ERL at Fern Hill in Canberra, with access to it by HQADF. Initially it could be limited to a capability of high data rate communications and (limited motion) video-conferencing, and could form part of a Telecom ISDN test network. Integration of such a testbed with the "Cooperative Communicating Networks" testbed research currently ongoing in collaboration with the USAFs Rome Laboratory (ex-RADC, Rome, NY) should be investigated.

7.5 Technologies and Tools Supporting the LCCS

The missions, functions, facilities and tools of the proposed C^{3}I Life Cycle Support System (LCSS) have been described in some detail in Section 5.5 and need not be repeated here.

In addition the development (or if such already exist, the evaluation and purchase) of **computer-aided tools <u>to manage</u> the evolutionary development of C^{3}I systems is a priority.** Such tools should be able to capture, generate, analyse, and maintain a high-level model of a subject C^{3}I system, which in conjunction with some inbuilt measures of performance, would simulate its operation and performance; at any point in time, it would need to incorporate within itself all the key features and key functionalities existing within the fielded (or approved) C^{3}I system it was representing.The **main objective of such a tool however would be to assess, at an early stage and at an indicative level only, the impact of any major proposed changes, growth, or additions in capability,** including the aggregated improvements for "Block" or "Mark $_{x+1}$" upgrades under EA, as shown on Figure 4. The tool/s should be graphically oriented for maximum communication and insight value. Any proposed changes would be inserted in a high-level, in a visual formalism and the model then activated, with the resulting C^{3}I system behaviour and performance indicating either (gross) improvements, or degradations or even system failure (or lack of (sub)system availability, or indications of potential problems with (sub)system integrity) and so on.

Such gross and early indications of the impact of proposed system changes is a most useful **risk management tool.**

Tools of this nature will draw heavily from information engineering developments, and would be designed with the very methods it is intended they support **(THO87).** Such tools have some affinity with KBSA (Section 6.1.2.3) as well as with another tool being developed at Rome Laboratory, the "Activity Coordination Formalism Design" **(SMP90).** The objective of the latter is to design a visual formalism for representing complex process models, and using them directly for describing and coordinating activities and communications in large scale software system development projects and systems acquisition. In the brief reference to it in **(SMP90),** its intended users, as well as its nature, are clearly identified with KBSA.

8 C^{3}I Architecture

8.1 Definitions

An universally accepted and yet precise definition of "architecture" (as in C^{3}I "architecture") is elusive. Generally, "architecture" implies a **specification** which describes how something (in this case the C^{3}I system) is constructed and interconnected, and includes any decomposition into functional modularity, as well as the interfaces and protocols which permit interworking, cooperation, and communication among its constituent modules (or subsystems). **Architecture is thus the specification of structure and connectivity; it is independent of the technology used.**

A more detailed, (NATO) C^{3}I-specific, definition of architecture is **(COM89)** :

> ..."(Architecture) is the description of the software and hardware structure of the (C^{3}I) system described in a number of documents, each detailing in formal statements (with an explanation of each statement) the technical structure of the system together with its functionalities"....

The role of architecture is that it specifies a structural framework which, when followed, permits a team of diverse stakeholders, with inevitable staff turnover, and using tools, techniques and materials which are changing and improving with time, to build and evolve, with consistency and economy, a (C^{3}I) system which is compliant with its original goals and missions, but which also encourages growth, extendability and improved capability, over a whole life-cycle of some 15-20 years.

8.2 C^{3}I Architectures

Architecture has connotations of "system structure", "functionality", "modularity", "connectivity, interfaces and protocols". "Achievability" and "implementability" must also be demonstrated. With so many attributes, it makes sense to define several parallel levels of architecture, rather than embody them into one. The following are the three C^3 parallel architectures adopted by NATO for their C^3 Master Plan (NATO , for their own reasons, omit "Intelligence" from C^{3}I) **(KER88)** :

(1) C^3 **Functional Architecture** : This is derived from agreed (NATO) C^3 doctrine and contains the required (NATO) C^{3}I functionality. By means of a C^3 structured analysis methodology called "Mission Oriented Approach"(MOA), linkage is made between (NATO) "mission components" and (NATO) "military functions". A common framework for discussing and formulating C^3 functions is thus provided as well as traceability of such functions (and hence of C^3 system capabilities) to (NATO) objectives and doctrine.

(2) C^3 **System Architecture** : This is the C^3 system decomposed (in the NATO case) into its four (sub)systems : the "Sensor and Warning Installation System" (which corresponds to our SICS); the "Information System" (which corresponds to our IOFIS); the "HQ and Facilities System" (which corresponds to our CSS); and the Communications System (which corresponds to our CS). (In our proposed system we have also included a C^{3}I Life-cycle Support System (LCSS)). Included in C^3 System Architecture are the specified software, security, communications etc architectures.

(3) C^3 **Management Architecture** : This defines the strategy, methods and milestones to transition or "migrate" from the present existing "baseline C^{3}I system" to the goal C^{3}I system defined by the previous two architectures, as a function of time, activity and resources. Included therein are any engineering and technical constraints, as well as any current, or anticipated technologies, which are expected to impact on, or even govern, the transition/migration process.

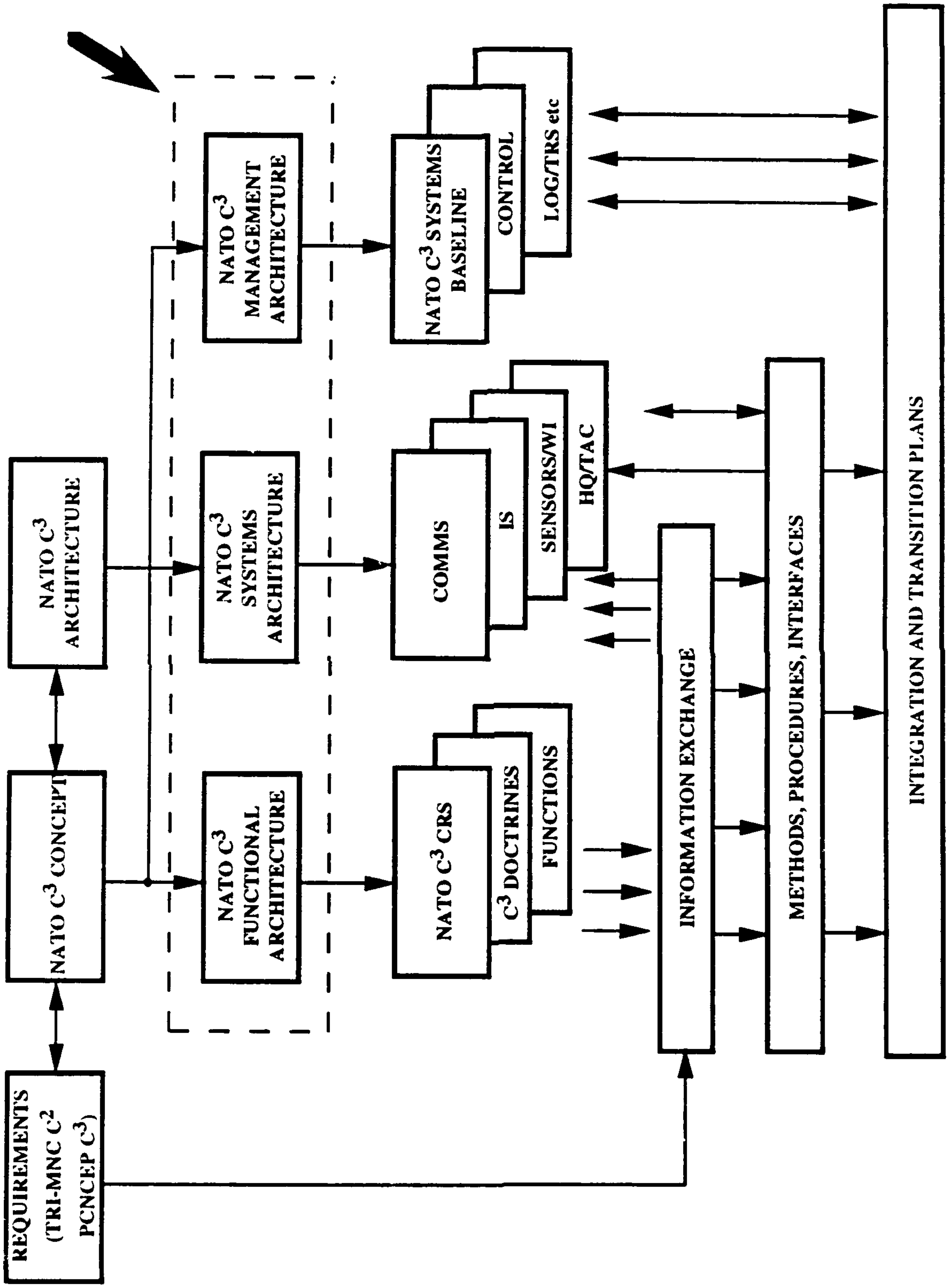

REQUIREMENTS (TRI-MNC C2 PCNCEP C3)
NATO C3 CONCEPT
NATO C3 ARCHITECTURE
NATO C3 FUNCTIONAL ARCHITECTURE
NATO C3 SYSTEMS ARCHITECTURE
NATO C3 MANAGEMENT ARCHITECTURE
NATO C3 CRS
C3 DOCTRINES
FUNCTIONS
COMMS
IS
SENSORS/WI
HQ/TAC
NATO C3 SYSTEMS BASELINE
CONTROL
LOG/TRS etc
INFORMATION EXCHANGE
METHODS, PROCEDURES, INTERFACES
INTEGRATION AND TRANSITION PLANS

Figure 5. NATO C^3 Architecture Components (from KER88)

Figure 5 shows these NATO C^3 architecture components and their relationships.The figure indicates that the first step in the logical sequence of arriving at these architectures begins at (C^3) "Requirements" which state and justify the **high level military requirements for C^3.** From this, a "C^3 Concept" is formulated from which the Functional Architecture is derived, based on the "mission oriented approach" and taking into account the (NATO) Orbat, and C^3-related capabilities and deficiencies. A C^3 doctrine and policy is formulated and C^3 functions defined.

The "C^3 Concept" leads to the "C^3 Architecture", which is refined as a" C^3 System Architecture" and decomposed into its four main (sub)systems, listed above, together with the associated "software", "security", "communications" etc, architectures.

The last, "Management Architecture" requires, in the first instance, a census of existing (NATO) C^3 systems to determine the Baseline Systems, the identification of any technical and engineering constraints, a Migration strategy, and Implementation Plans between major milestones to achieve this.

Refinement of each of the detailed implementations occurs throughout this process, and is explicitly indicated by the interaction and information arrows between the constituent entities. Figure 5 thus shows not only the architectural relationships but also the process. The development and acquisition will be carried out by Evolutionary Development and Acquisition.

It must be noted on Figure 5 that **the architectures are fixed and are not subject to change.**

8.3 C^3I Layered Architecture Principles

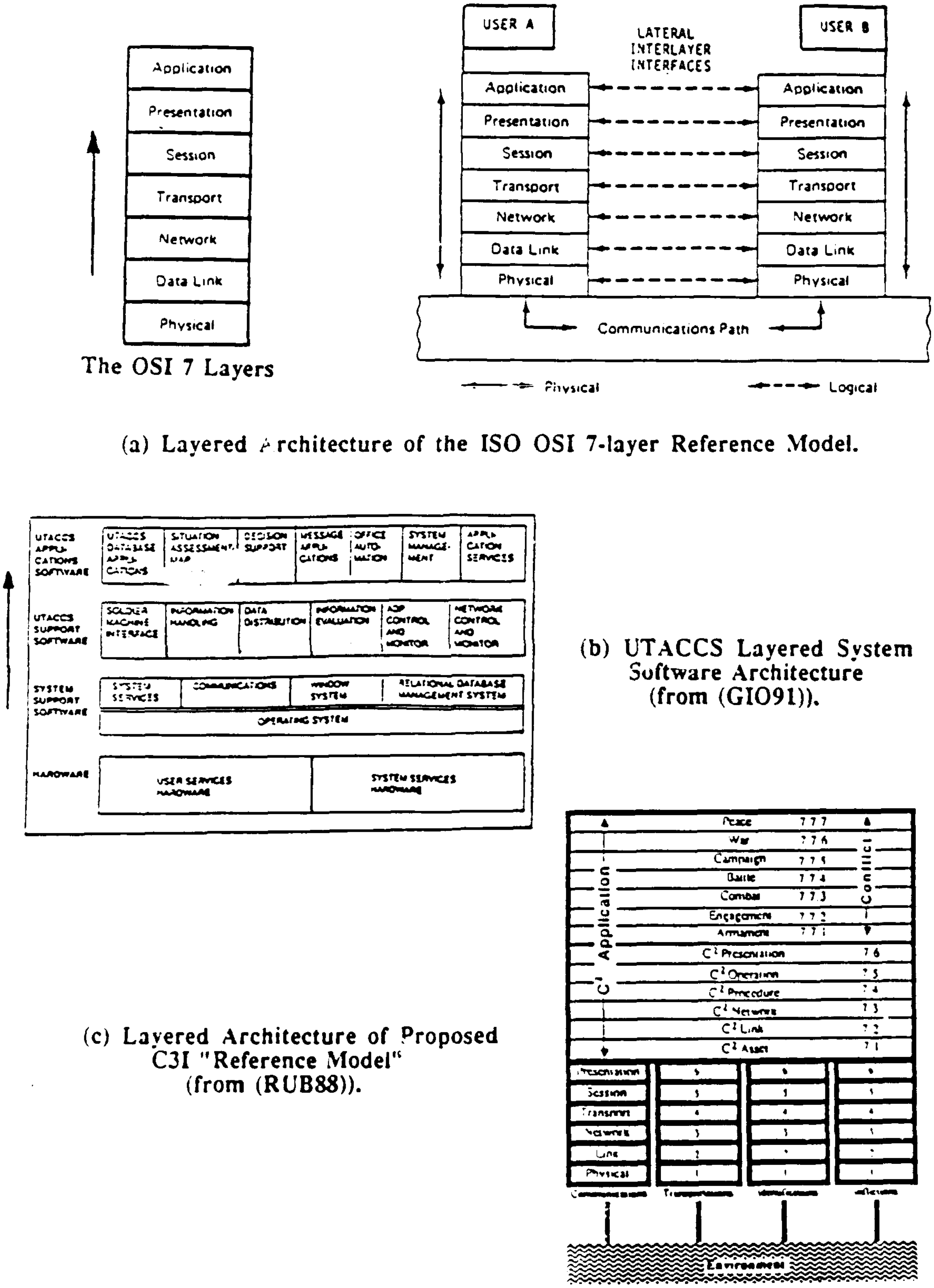
Several specific architectures have been referred to and briefly described, in particular the UTACCS software architecture (section 6.1.2.6) and the architecture for heterogeneous platform intercommunications based on the ISO OSI 7-layer reference model (section 6.1.2.7). The common feature of both these architectures is that they are based on the **principles of layering**, wherein the components of the process (in the examples given, the software implementation and communication processes) are grouped in an hierarchical arrangement in such a manner that the **lower layers provide functions and services that support functions and services of higher layers (WEI83).**

Figure 6 in particular shows these examples in a schematic form. Figure 6(a) shows the OSI 7-layer architecture, implementing the data communication process, between two end users (computers), divided into seven functionally separate and well defined steps. **Associated functions are assembled in one layer**, which includes a module for layer management; the function of this module is to set parameter values and compile error statistics. Connectivity is established by successive layer-to-layer communications which transmit protocols, which through administrative procedures, govern each of the seven layers.

The UTACCS software architecture layers(see Section 6.1.2.6), in Figure 6(b), provide a specific set of services and C^3I applications, while isolating the lower-level implementation details.

Implementation of both communications and computer systems, the two technologies which underpin C^3I, is very amenable to layered architectures. Systems can be built of ever-increasing capability, by superimposing layers one above the other, or by adding layers below to improve existing capability, with each layer using the facilities below and supporting the layer above. Thus the layered architecture concept permits using components that are already in place, while still improving the capability of the overall system. Consequently, **the layered architecture principle is optimum for the architecture required fcr systems undergoing evolutionary development.** It is likely however that some reduction in performance, specifically in processing speed, could occur.

A framework for defining the C^3I process, spanning many C^3I-related resources has begun to be investigated and explored through layering principles, in particular by their application in building a C^3I "reference model" (or perhaps a number of interlinked reference models). One objective of this is to explore how the resource aspects (surveillance sensors and systems, communications, materiel, personnel and associated logistics, and weapon system assets) may drive the design and implementation of a C^3I system (**RUB88, HOL87, HOL88**).



The OSI 7 Layers

(a) Layered Architecture of the ISO OSI 7-layer Reference Model.

(b) UTACCS Layered System Software Architecture (from (GIO91)).

(c) Layered Architecture of Proposed C3I "Reference Model" (from (RUB88)).

Figure 6. Architectures Based on Layering Principles

Figure 6(c) shows, in broad detail, such a proposed layered architecture for the C^3I process (**RUB88**). It is an attempt to subdivide into a number of well-specified, robust sub-processes the broadest description of the C^3I process, given in Section 3.1, namely that C^3I is about the management of resources to achieve a given objective. The proposed layered architecture is based on, and is an extension of, the 7-layer ISO OSI reference model, but with three additional parallel sets of processes interacting through a number of common applications layers, as well as through the **environment.**

The set of four interacting processes is :

(a) **Identification** : These are interactions which result directly in the recognition of objects in the environment. In the basic C^3I paradigm shown in Figure 1, this corresponds roughly to "observation" (and includes "identification").

(b) **Communication** : These are interactions which involve the exchange of information and which effect command, control and coordination between resources. In Figure 1 these are essentially the arrows interconnecting the various blocks.

(c) **Transportation** : The interactions and the process to carry, supply, equip, etc. the resources ("own forces") with materiel, and personnel.

(d) **Infliction** : The process and interactions which destroy, damage, degrade, or disrupt (hostile) objects.

Both (c) and (d) together correspond to "action" in Figure 1.

In lieu of the top "application layer" in the ISO 7-layer model, two additional groups of layers are provided to complete the interactive C^3I process (thereby describing this process by a group of three "super-layers"). The uppermost "super-layer", consisting of seven layers, is called the "conflict layer" and concerns itself with the levels of conflict being managed by the C^3I process. The lower applications "super-layer", consisting of six layers, deals with the command and control aspects trying to resolve the given conflict. It is this middle "super-layer" of C^2 applications that corresponds to the "decision" element of the C^3I basic paradigm shown in Figure 1.

It is outside the scope of this report to describe the details of the C^3I interactions under this proposed C^3I "reference model"; details are given in (**RUB88).**

A similar layered architecture approach, with the objective of providing an automated Command/Battle Management/Combat Direction system, is described in **(HOL87, HOL88).**

8.4 C^3I System Development Architecture

Figure 7 shows, in "architectural block" diagram form, the proposed C^3I "system development architecture".

The development of any ADF C^3I system will rest on a "base" of "Evolutionary Acquisition" (EA), which includes "Evolutionary Development", the development component of EA.

Immediately above this supporting base is the physical supporting structure for C^3I development, the "C^3I Life-cycle Support System", common to, and shared by, all future ADF C^3I systems.

Each operational C^3I system will consist of the four major (sub)systems namely, the Communications System, based, wherever possible, on ISDN and Broadband-ISDN; a Command Support System; an Intelligence and Information System; and a Surveillance and Information-collection System.

All C^3I systems will be implemented by Open Systems wherever possible; but this needs to be balanced by an appropriate global C^3I system security architecture.

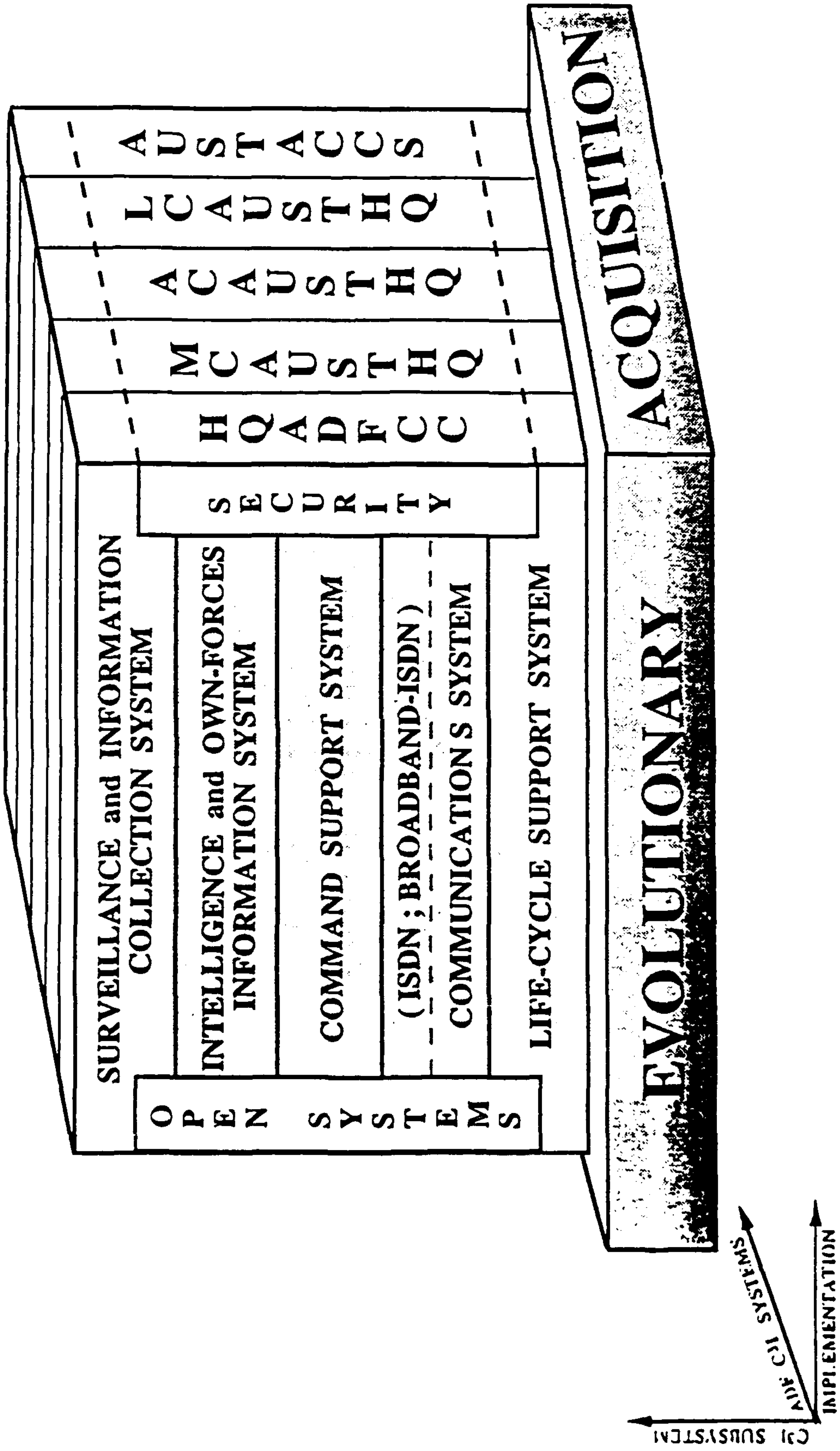


Figure 7. C^{3}I System Development Architecture

Finally, the same architecture, with the same supporting elements, will eventually apply to all ADF C^3I systems or subsystems, as exemplified in Figure 7 by the ADFCC at HQADF (JP 2030), the various systems for the Maritime, Air, and Land Commanders, and possibly to AUSTACCS in some future configuration as well.

8.5 Proposed C^3I Goal Architecture

Figure 8 indicates a proposed C^3I goal architecture based on layering principles.

The C^3I system is supported by, and rests on, the bottom "communication layer(s)" enabling, on the one hand, communications between the C^3I system and own forces, allies, the geographically dispersed sensors and surveillance assets, and cooperating agencies whether national or of allies; and on the other hand, communications internal to the C^3I system between its own (sub)systems and elements.

Above this bottom communications layer is the "information systems layer", consisting of sublayers of hardware and C^3I system support software (communications, data base management systems, window systems and other common system services), all, wherever possible, Open Systems-compliant, and aggregated into localised "information systems" (in the most general sense), each such information system interlinked via a local area network (LAN).

The information systems layer(s) support the remaining three C^3I (sub)systems, the SICS, the IOFIS and the CSS, each of which has its own "(sub)system-specific support layers" (specific database management systems, data distribution, man-machine interfaces etc), and the "(sub)system-specific applications layer(s)".

All layers are supported by a consistent (multi-level) security architecture, and a management (of C^3I system development) architecture.

Above the whole are the C^3I system users.

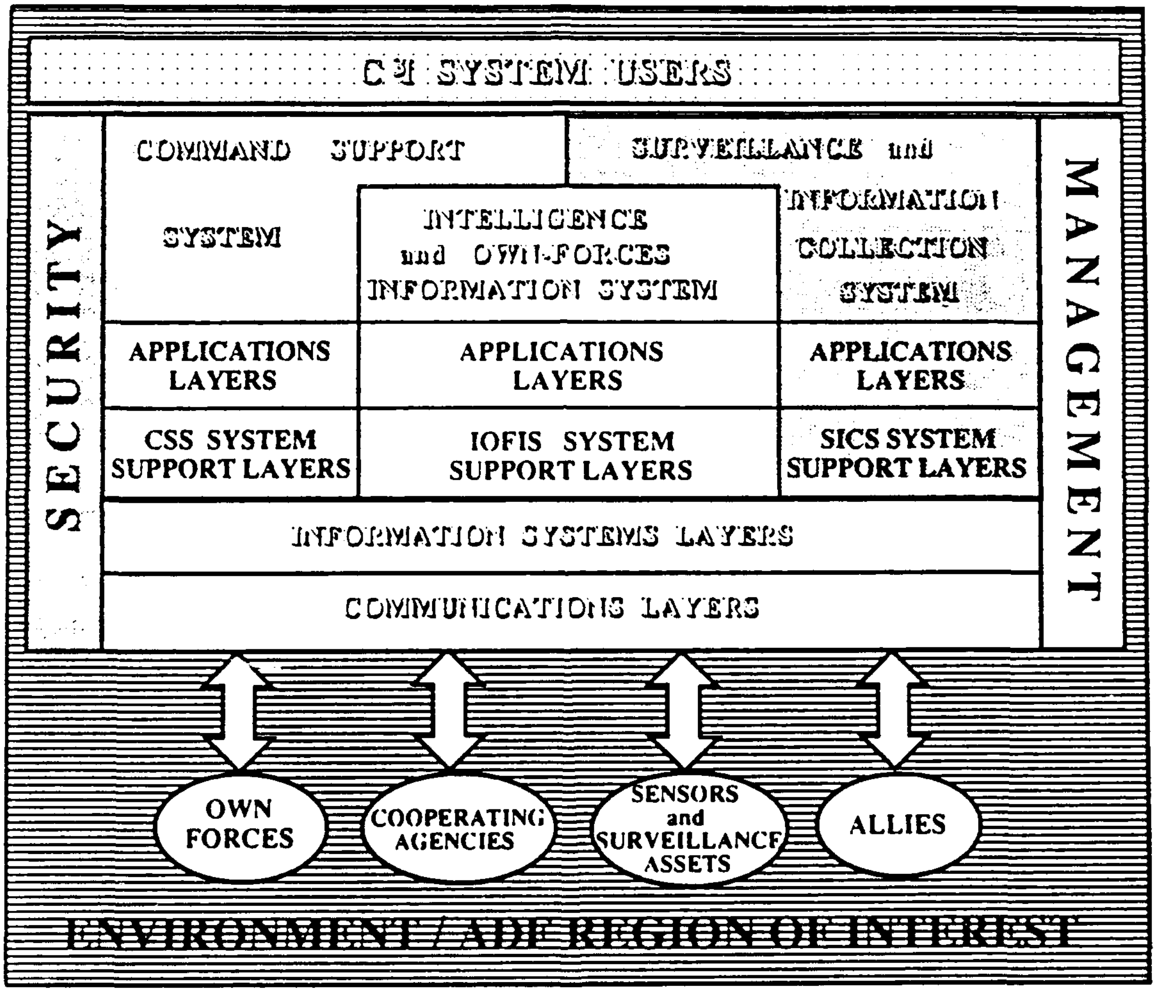

C3I SYSTEM USERS
COMMAND SUPPORT SYSTEM
SURVEILLANCE and INFORMATION COLLECTION SYSTEM
INTELLIGENCE and OWN-FORCES INFORMATION SYSTEM
APPLICATIONS LAYERS
APPLICATIONS LAYERS
APPLICATIONS LAYERS
CSS SYSTEM SUPPORT LAYERS
IOFIS SYSTEM SUPPORT LAYERS
SICS SYSTEM SUPPORT LAYERS
INFORMATION SYSTEMS LAYERS
COMMUNICATIONS LAYERS
SECURITY
MANAGEMENT
OWN FORCES
COOPERATING AGENCIES
SENSORS and SURVEILLANCE ASSETS
ALLIES
ENVIRONMENT / ADF REGION OF INTEREST

Figure 8. Proposed C^3I Goal Architecture

9 C^{3}I Migration Plan

9.1 General Comments

A C^{3}I **Migration Plan** need be integral with a C^{3}I Master Plan, which it is anticipated will follow on from a C^{3}I Strategic Plan. It is the document which would detail the nature of, and sequence, schedule and resources required for, improvements in performance and growth in capability to be incorporated into existing or planned ADF C^{3}I systems, to transition them from their existing operational capability, in phased stages, to the state-of-the-art C^{3}I systems envisioned in the C^{3}I Strategic Plan. The Migration Plan must be compliant with the C^{3}I Strategic Plan and must be endorsed and approved by the stakeholders of the respective C^{3}I systems it applies to.

The role of the Migration Plan is to provide the route, and the directions needed to follow that route, along which the Evolutionary Acquisition of any particular ADF C^{3}I system will progress.

The prerequisites for a C^{3}I Migration Plan are that :

(1) a C^{3}I Strategic Plan, with a follow-on ADF C^{3}I Master Plan with a C^{3}I goal architecture, have been prepared and approved;

(2) the capabilities (and deficiencies) of the current and planned ADF C^{3}I systems, as well as the capabilities (and deficiencies) of the other major C^{3}I (sub)systems (SICS, IOFIS, Communications etc or their current equivalents) have been assessed in the C^{3}I Master Plan context, and their "baseline" configurations and capabilities defined; and

(3) that the proper goals and missions, and hence the requirements and functionalities of, the individual ADF C^{3}I systems have been endorsed and approved.

From the foregoing in this report, this is clearly yet to be done; specifically, the kind of process, and the products from such a process, as outlined in Section 7.2 and carried out by NATO, or something similar to it, needs to be carried out by the ADF, which will then produce C^{3}I Functional, System and Management Architectures appropriate to ADF C^{3}I.

The clear conclusion is that at present **a comprehensive and complete C^{3}I Migration Plan cannot be prepared at this stage.** Indeed attempting to do so, would be to go against the very advice developed to date in this Report. A comprehensive Migration Plan itself is to be prepared after both the C^{3}I Strategic Plan and ADF C^{3}I Master Plans have been drafted, in consultation with all C^{3}I stakeholders. However, the processes and activities required to develop and prepare such a Plan will be identified. As well, the initial "steps and directions", in the form of a number of Recommendations, considered necessary to support both C^{3}I Strategic and Master Plans, and hence the Migration Plan, are given at the end of this Report, in Section 11.

These Recommendations may be considered to form the first steps towards a C^{3}I Migration Plan.

9.2 Activities Required to Support the C^{3}I Migration Plan

Firstly, the concept of a C^{3}I Strategic and Master Plans needs be endorsed by the major ADF C^{3}I stakeholders, and such Strategic and Master Plans, to include the C^{3}I system, software, security, communications etc, architectures, then prepared. The following activities will need to be carried out :

(a) A "census" of existing and planned ADF C^{3}I systems is required; in practice this means the Command Support Systems (CSS) proposed or in planning for the MCAUST HQ, ACAUST HQ, LCAUST HQ etc. The initial/"baseline" operational capability (IOC) of each needs be determined and defined, and existing deficiencies identified. Compliance, or amenability, of each C^{3}I system to the proposed C^{3}I goal architectures needs be assessed; as well as an assessment of their existing, or amenability to, interoperability with intra-national/inter-Service C^3I systems in the first instance, and, secondly, with inter-national/Allied systems.

A similar census of the major C^3I (sub) systems, specifically of surveillance and information collection assets and their equivalents (ie the SICSs); of the Intelligence and Information Systems and their equivalents; of the communications system, its civil infrastructure, plans and implementation schedules etc; to determine their capabilities, and to identify and characterize any deficiencies, need to be carried out.

The above censuses and resulting assessments and studies will enable the ADF C^3I Baseline Systems to be defined.

From the defined ADF C^3I Baseline Systems, any deficiencies in C^3I capabilities may be identified and endorsed by the end-user and other stakeholders of the C^3I system in question. The C^3I requirements and functionalities should then be refined, redefined and endorsed.

(b) A comprehensive or "master" C^3I Migration Plan may then be developed to encompass all ADF C^3I systems. This should include :

(i) Identification and characterization of the capabilities and functionalities common across all ADF C^3I systems, as well as the identification and characterization of single-user C^3I system peculiarities.

(ii) Identification and prediction of anticipated developments in C^3I system capabilities in general, and, in particular, based on likely developments in the civil/commercial market place, in the areas of Open Systems, COTS, and ISDN, B-ISDN, and any other longer-term civil sector telecommunications developments.

(iii) Identification of, and likely implementation sequence, plan and schedule, for the C^3I planned improvements common to the majority of (or all) ADF C^3I systems

(iv) Description of the Evolutionary Acquisition methods and processes to be used.

(v) Identification, and means of implementation, of the computer-based C^3I development and management environment.

(vi) Identification of any technical risks, and other technical and implementation constraints, which may impact on the Migration Plan , schedules, costs etc.

(c) "Individual" C^3I Migration Plans and schedules need be developed to migrate specific C^3I systems, which are compliant with, or amenable to, the C^3I Architectures in the Master C^3I and Migration Plans, to their endorsed envisioned configuration, based on a schedule of phased prioritized and achievable improvements, and consistent with the broad "Master" Migration Plan. This needs be done in consultation with, and with the agreement of, the C^3I system end-users.

(d) These "Master" and "Individual" C^3I Migration Plans need to be periodically reviewed to accommodate unforeseen technological developments as well as changes to C^3I operational requirements which reflect command and Force Structure changes, and changed as necessary, provided these are consistent with, and are permitted by, the C^3I architectures.

After all, over the 15-20 years whole-life cycle of C^3I systems, the Master Plan itself, as well as its management and implementation, must be flexible enough to be subject to evolution themselves!

9.3 C^3I Migration Plan Initial Recommendations

Although this Report is a start to the C^3I Strategic Plan, the Plan itself is still a proposal only at this stage. An appropriate C^3I organization and infrastructure must be endorsed and set up to carry out the processes which have been identified in this report, and which will be fully specified in the C^3I Master and Migration Plans. Staff and facilities to carry out, effect and implement the Migration Plan need be acquired, trained and coordinated.

Recommendations to put the above in place, 33 in all, are given in Section 11, and hence will not be repeated here. They fall in five distinct classes, relating respectively to:

(1) the overall C^3I Master Plan;

(2) the building up of an C^3I infrastructure;

(3) C^3I Goal Architectures;

(4) C^3I tools and methods:

(5) C^3I near-term tasks and activities.

These Recommendations in essence make up the initial part of the C^3I Migration Plan.

9.4 Longer-term C^3I R&D Activities

It is worthwhile to identify and flag at this stage some of the longer-term R&D activities necessary to support the evolution of C^3I. Some of these follow directly from Section 4, 7 and 8.

R&D areas include :

(a) **C^3I Systems Theory and Systems Engineering.**

(b) **C^3I Architectures,** in particular, to develop **a layered system architecture,** to reflect the detailed C^3I process interaction between the C^3I system end-user and any part or (sub)system of the C^3I system to support the C&C function, by subdividing the process into robust and well-defined sub-processes, and associating each with a "layer", which in turn can be automated, and which has well defined interfaces with the adjacent layers below and above it.

(c) **The development of methods and tools to build efficient, reliable and affordable C^3I software consistent with evolutionary development and acquisition and in particular to investigate object-oriented methods to accomplish this.**

(d) **Methods for developing and integrating National Surveillance, Information Collection, Intelligence Collection and Intelligence Plans into C^3I, in forms which lend themselves to rapid amendment** (possibly based on AI-based Mission Planning Aids methods).

(e) **Multi-source Information Fusion,** to generate situation assessments, under conditions of incompleteness of data, presence of high noise levels and imprecision, uncertainty, and, in times of tension and conflict, under conditions of deliberate mis- and dis- information.

(f) **Multi-media databases** : their nature, requirements, structures, query-and-access problems, and their update and general management and **the applicability of third-generation object-oriented databases for this.**

(g) **C^3I Measures of Effectiveness and C^3I System Evaluation Criteria.**

(h) **Optimum C^3I Information presentation,** for Administration, Operations, Force Structure etc applications.

(i) **"Groupware"/"Lifeware" for C^3I.** "Groupware" or "lifeware" are computer-mediated and supported tools, techniques and methods, which specifically support and augment group work, such as design, planning, decision-making etc, by groups whose members are either locally or widely and geographically dispersed.

(j) **Command and Control processes, decision-making, and effectiveness under information overload and stress.**

Capabilities and facilities to carry out this work exist in ITD and CD of ERL.

10 Conclusions

The following are the conclusions from preliminary considerations of the C^3I Strategic Plan:

(1) C^3I is beset with uncertainty and complexity, much of it arising from the incomplete definition of requirements.

(2) By their inherent nature, C^3I requirements cannot be specified completely ab initio but, rather, evolve with time as :

(a) the C^3I process becomes refined and better understood;

(b) the C^3I system grows and its capabilities evolve to meet the changing threat and changes in national and ADF priorities;

(c) innovations and developments are made in C^3I-associated technologies.

(3) Evolutionary Acquisition (EA) is the strategy through which these C^3I-associated difficulties can be, and have been, successfully overcome.

(4) Any ADF C^3I Master Plan, and in particular its associated Migration Plan to transition from current/existing C^3I systems to modern state-of-the-art systems, must rest on EA.

(5) The first step to that end needs be the acceptance of EA for C^3I systems by all C^3I stakeholders, to be followed by the creation and acceptance of an organisation to manage and implement this, with membership drawn from the key C^3I stakeholder organizations, specifically from HQADF as the main C^3I system sponsors, individual uniformed Services as C^3I system co-sponsors and end-users, DSTO as C^3I systems R&D authorities, co-developers and system testers, and appropriate contractors as C^3I systems co-developers and builders.

(6) A generic C^3I system has been described, the major subsystems of which are common across a number of existing and proposed ADF C^3I systems. The generic C^3I system integrates Surveillance and Intelligence assets and processes with Communications and the Command and Control function, with its associated decision and planning aids.

(7) A key C^3I subsystem, necessary to its successful development and maintenance of any C^3I system over its whole life-cycle - which may typically be of the order of 15-20 years - is the C^3I "Life-cycle Support System" (LCSS). Its mission and objectives are given in Section 5.5.

(8) The necessary tools, techniques and processes to support EA are either available or are in advanced development, and brief descriptions are given.

(9) Because of the evolutionary nature of C^3I systems, as well as their lengthy whole life-cycle, C^3I architectures should be based firstly on the principles of "layering", and secondly on Open Systems Standards, to prevent single-vendor lock-in, and to obtain and maximize the leverage and benefits from civil/commercial sector developments and from multi-vendor systems.

(10) Current and future civil communications infrastructure, in particular the Integrated Services Digital Network (ISDN) and its follow-on, Broadband ISDN (B-ISDN) will match well, and can provide the bulk of, the communications for existing and future ADF C^3I systems. These, however, will need to be complemented by a leaner, but dedicated to C^3I systems only, Defence-owned communications system.

(11) The development of a C^3I Strategic Plan, and its follow up ADF C^3I Master Plan and their acceptance by C^3I stakeholders will, in their early phases at least, need be evolutionary as well. To that end, a number of specific recommendations (the following Section) have been made.

11 Recommendations

ᵎ ie following form the Initial Recommendations of the Migration Path of the C^{3}I Strategic Plan.

11.1 Recommendations Relating Overall to C^{3}I Strategic Plan

1. That the concept of a C^{3}I Strategic Plan and a follow-on ADF C^{3}I Master Plan to direct the development and acquisition of current and future C^{3}I systems for the ADF be accepted by the key C^{3}I stakeholders and that any Master Plan be based on the strategy of Evolutionary Acquisition (EA).

   Key C^{3}I stakeholders need be identified, but, in the first instance, will include:

   (1) HQADF, in particular Development Division as C^{3}I main sponsor, and Operations Division as C^{3}I main user.
   (2) DSTO, in particular ERL, as C^{3}I R&D authority and C^{3}I systems tester.
   (3) Individual uniformed Services, as C^{3}I systems co-sponsors and end-users.
   (4) Defence Acquisition and Logistics Organisation, in particular Project Development and Communications Division.
   (5) Contractors of individual C^{3}I systems, as C^{3}I system builders, and as required.

2. That an Interim C^{3}I Steering Committee be set up, with membership drawn from the key C^{3}I stakeholder organizations, and tasked with setting up the organization structure necessary to manage and impiement EA for ADF C^{3}I systems, and to agree on the necessary operating processes and membership composition of the permanent organization.

11.2 Recommendations Relating to Building-up C^{3}I Infrastructure

3. Establish as soon as practicable a formal relationship between ERL and the HQADF authority on C^{3}I policy and doctrine; or in the absence of such an authority, recommend to appropriate HQADF authorities the need to create such a position.

4. Identify and implement an appropriate organization within ITD and CD of ERL to manage and implement DSTO C^{3}I activities, and in particular evaluate a C^{3}I matrix management structure (ie C^{3}I technologies vs. C^{3}I products) as a candidate for this.

5. Identify and implement mechanisms to ensure wide distribution of C^{3}I planning and implementation documents and reports (sanitized wherever necessary) to Australian industry (and academe) to assure their interest and facilitate their subsequent entry as C^{3}I stakeholders as early as possible.

6. Through consultation between all C^{3}I stakeholders, identify and select personnel to participate in, and implement processes to influence, international Standards bodies and committees, in particular within ISO and CCITT relating to Open Standards, ISDN and B-ISDN, to influence such standards to meet Defence and C^{3}I needs and requirements.

7. Identify, formalize and strengthen any existing links, and as necessary develop new links, with Telecom (and any other, future Australian telecommunications entity) to influence the development of the civilian national telecommunications infrastructure and capabilities, to meet Defence needs in general, and those of C^3I in particular.

8. Identify existing or potential bilateral and multilateral agreements with our Allies, under which suitable C^3I joint RDT&E activities could be undertaken; identify specific candidate activities; pursue as necessary new collaborative agreements and mechanisms if necessary; pursue and implement such collaboration whenever benefits are clearly identified, and quantified if possible.

9. Identify suitable candidates, and implement wherever possible the following, for developing and widening the in-country C^3I technology base, including the following :

   (a) sponsor visits by overseas C^3I authorities to present short, intensive C^3I courses at DSTOS, Canberra and Sydney;

   (b) send selected staff from DSTO and other stakeholder organizations on long term overseas attachments to appropriate defence, research, academic establishments and user installations;

   (c) encourage research in in-country industry and academe in C^3I related areas.

11.3 Recommendations Relating to C^3I Goal Architecture

10. In developing goal architectures for C^3I and their associated system, software, communications, security etc architectures, use the "principles of layering", where components and related functions are grouped in a hierarchical arrangement of layers, with the lower layers providing functions and services that support the function and services of the adjacent higher layer. This approach lends itself well to evolutionary development by the process of adding additional intermediate or higher layers to improve capability, with each such layer using the facilities below it and supporting the layers above it.

11. Use wherever possible and appropriate non-proprietary, multi-vendor systems compliant with Open Systems Standards. The use of Open Standards non-compliant systems and hardware is not excluded but the cost-benefits of their use must be argued and documented.

    Specifically for computer data and information communications and interworking, an appropriate GOSIP (Government OSI Profile) of standards needs be established, based on the ISO OSI (Open Systems Interconnection) 7-layer Model, and tailored to enable the basic and necessary C^3I systems functions, including data communications, e-mail, transmission of standard-formatted documents, and data base access and query.

12. The longer term vision for Open Standards in C^{3}I is for their applicability to span across all of C^{3}I, from enabling connectivity between multi-vendor and heterogeneous computer systems, through user transparent operating systems (possibly based on or derived from Unix), through C^{3}I-common applications software such as e-mail, word processing, data base management systems, and graphics user-machine interfaces (possibly based on X-Windows, which currently seems to be the de-facto Industry standard or the more general OSF/Motif, currently being proposed as the user interface standard), to specific applications such as mission planning and decision aids, etc.

13. Wherever possible and whenever available, commercial-off-the-shelf (COTS) software, applicable to C^{3}I and compliant with Open Standards, should be purchased, evaluated against C^{3}I requirements, and if found suitable, incorporated in the appropriate C^{3}I system.

14. Evaluate, and apply in C^{3}I systems, as they are developed and accepted, any Open Standards which promote the following desirable properties :

    (a) Compatability : applications running on a given or current system, must be able to run future (software) releases.

    (b) Portability : applications running on a given hardware platform must be able to run on any vendor's platform of the same or similar class.

    (c) Scalability : applications should run on a full range of systems architectures from laptops to mainframes.

    (d) Interoperability : systems must be able to interoperate, and interwork, on shared data and information.

15. To meet the requirements of the Defence Communications Strategic Plan, to encourage the implementation of Open Standards, and to provide for the interoperability between lateral and with Allied C^{3}I systems, utilize and leverage on civil sector telecommunications and its infrastructure for the bulk of C^{3}I communications, initially for voice, data and information transfer, and later on for video and imagery and other high bandwidth requirements, in particular, by utilizing the currently-being installed ISDN (Integrated Services Digital Network), and its follow-on, fibre-optics based, Broadband-ISDN (B-ISDN).

16. Means and mechanisms need be explored and implemented to have inputs into, and influence over, the ISDN- and B-ISDN-standards formulating committees in the respective ISO and CCITT bodies and committees, to assure that C^{3}I requirements are included in the appropriate standards. This can be done through either Defence or C^{3}I stakeholders membership, or through current Australian delegates to these bodies.

17. Retain and as needed, develop, a lean and, necessarily, a less capable Defence-owned communications system for backup and emergencies.

18. A C^{3}I global information security architecture needs be developed and implemented. Such a security architecture :

(a) must incorporate multi-level security;

(b) must be encompassed within the ISO OSI 7-layer model and Commercial-off-the-shelf (COTS) environments;

(c) must address all aspects of "information warfare" counter-countermeasures, in particular communications security, computer security, and information and software security.

11.4 Recommendations Reiating to C^{3}I Tools and Methods

19. Because they lead to quality software development and support evolutionary development, investigate object-oriented methods for analysis, design, programming, and testing, and implement as early and as widely as possible, to assure "seamless" transitions between each of these C^{3}I system development phases. Investigate, evaluate and implement as appropriate Object-oriented Databases (OODB).

20. For software development, use the Ada programming language as necessary and appropriate. Although not a true object-oriented language, Ada is amenable to, and compatible with, this approach.

21. Use non-procedural programming languages where applicable, in particular for expert-system applications such as planning aids, decision aids, for some specific classes of data bases, etc.

22. Develop and implement a methodology for justifying and recording specific C^{3}I requirements and functionalities by relating them to military (and other authorized) missions and functions, and recording the linkage and traceability between these.

23. Investigate and evaluate IPSE's (Integrated Project Support Environment) for the management of C^{3}I system development, and in particular for C^{3}I software development. Assess for suitability the KBSA (Knowledge Based Software Assistant) as a machine-mediated and supported tool to aid the C^{3}I requirements capture, documentation, and traceability, as well as an expert-based tool to suggest plausible strategies for the design of software and program modifications, and to perform Software Development Management functions. Monitor the progress in Information Engineering and Systems Engineering methods and tools and their applicability to C^{3}I system development, in particular to the IOFIS.

24. Investigate, evaluate, and assess the suitability of existing C^{3}I software architectures, commercially developed by object-oriented approaches, as a skeletal framework for modification and adaptability for ADF C^{3}I systems.

25. Establish within ERL a C^{3}I Life-cycle Support System with missions, objectives, and facilities as described in Section 5.5 of this Report.

11.5 Recommendations Relating to C^{3}I Near-term Tasks

On acceptance of Recommendations 1 and 2 in Section 11.1 above :

26. **Begin the implementation of Recommendation 25, relating to the setting up within ERL of the C^{3}I Life-cycle Support System.**

27. **Begin the implementation of Recommendations 3-9, relating to the building up of a C^{3}I infrastructure.**

28. **Review the elicitation of C^{3}I requirements process existing and applied to date in-country; compare with proposed processes overseas, including rapid and exploratory prototyping. Begin work towards formalizing and implementing the preferred requirements elicitation and capture process, in particular its documentation and traceability to C^{3}I policy and doctrine.**

29. **Begin the census of ADF existing and planned C^{3}I systems, their current and planned missions and objectives, requirements, functions, capabilities, implementation and status, to determine and characterize their baseline capabilities. Therefrom begin drawing up with stakeholders the individual migration plans to state-of-the-art C^{3}I systems. Examine all for de facto obsolescence, future non-supportability, and candidature for cancellation.**

30. **Begin a census of Surveillance assets, sensors and other information collection systems relevant to ADF C^{3}I, their current and planned missions and objectives, capabilities, implementation and status, to determine and characterize their system capabilities, data and information flows and rates etc. Integrate this with National Surveillance and Information-, and Intelligence-collection Plans to determine their system capabilities, characteristics, as well as any deficiencies, from a C^{3}I perspective.**

31. **With appropriately selected Information Engineering tools, methods and processes, and in agreement and collaboration with appropriate C^{3}I user organisations, determine and characterise a top-down view of ADF C^{3}I system requirements, in particular, by determining missions, objectives, functions, and information structures and flows of particular organisations.**

32. **Establish links, and consult, with the appropriate staff developing and promulgating C^{3}I doctrine, procedures and related tasks, at the ADF Warfare Centre (ADFWC), Williamtown, NSW.**

33. **Continue developing the C^{3}I Strategic Plan, which itself is an evolutionary activity.**

Acknowledgements

The author wishes to acknowledge the valued criticisms and comments of his colleagues in Information Technology Division, ERL, DSTO, during the preparation of this Report, in particular Drs. J. Aisbett, I. Chessell , S. Hood and Messrs. P. Calder, P. Deer, S. Landherr, J. Schapel and E. Youle.

THIS PAGE INTENTIONALLY LEFT BLANK

REFERENCES

(AAR91) Aaron, M.R., Decina M.,"Asynchronous Transfer Mode or Synchronous Transfer Mode or Both?", IEEE Communications Magazine, Jan. 1991, pps. 10-13.

(ABR89) Abramowicz, H., Lindberg, A., "OSI for Telecommunications Applications", Ericsson Review, No. 1, 1989, pps. 1-12.

(AIS91) Proceedings of "Advanced Information Systems : AIS91", 19-21 March, 1991, London: Learned Information (Europe) Ltd., Oxford, UK.

(AND89) Andrews, F.B. et al.,"Towards an Integrated Australian Defence Communications Architecture", Technical Report ERL-0484-TR, ERL, DSTO SAlisbury, Sept. 1989 (Confidential).

(AND90) Andrulis, M.W., "Object-Oriented Development Aids Prototyping and Delivery", Signal Dec 1990, pps.76-78.

(AFCEA87) "Information and Consultation: Keys to Peace", Proceedings of 8th AFCEA Europe Symposium, 21-23 Oct 1987, Brussels, Belgium: AFCEA, Washington, DC.

(AFCEA88) "New Technologies for NATO C^3I ", Proceedings of 9th AFCEA Europe Symposium, 18-20 Oct 1989, Brussels Belgium.: AFCEA, Washington, DC.

(AFCEA89) "Fulfillment of NATO C^3I Requirements", Proceedings of 10th AFCEA Europe Symposium, 24-26 Oct 1989,Brussels, Belgium: AFCEA, Washington, D.C.

(ASP90) "Australia's Strategic Planning in the 1990's", Dept. of Defence, Canberra, Oct 1990 (Secret AUSTEO), pps. 37 and 40.

(ATH87) Athan, M. "Command and Control (C^2) Theory: A Challenge to Control Science", IEEE Trans-AC, AC-32, 4, April 1987, pps. 286-293.

(ATW91) Atwood, T.M., "The Case for Object-oriented Databases", IEEE Spectrum, Feb. 1991, pps. 44-47.

(AUS88) "Tactical Command Support System : AUSTACCS', DD(X)5292, Issue 2, 30 Nov 1988 (Draft), Army Office, Canberra, 1988.

(AXI91) "Productivity Improvement Through Rapid Application Development, CASE, and Re-engineering", Seminar Notes by P. Mimno, May 1991, AXIS Technology Pty. Ltd., Sydney, NSW.

(BAR87) Barnes, D.,"Security Architectures for Information Systems", pps. 30-33 in (AFCEA89).

(BAR89) Barthes, J-P. A., Le Noan, Y.,"A Command and Control System Based on a Multi-media Object-oriented Data Base and a Logic Programming Language", Proc. "Annual *AI Systems in Government" Conference, 27-31 March 1989, Washington,* DC : IEEE Computer Society, pps.126-132.

(BES91) Best, D., "Impact of User Interface Technologies on Office System Strategies", pps. 83 87 in (AIS91).

(BOO86) Booch, G., "Object-Oriented Development", IEEE Trans-SE, Vol SE-12, No. 2, Feb 1986, pps. 211-221.

REFERENCES (continued)

(BOO87) Booch, G., "Software Components with Ada", Benjamin/Cummings, Menlo Park, CA., 1987.

(BUR90) Burrough, P.A.,"Principles of Geographical Information Systems for Land Resources Management", Monograph on Soil and Resources Survey No. 12, Oxford Science Publications, UK, 1990.

(COH87) Cohen,A.,"Data Telecommunications : Developing a Security Architecture", Proceedings of IEEE INFOCOM'87, IEEE Press, NY, 1987, pps. 693-698.

(COM89) Complin, B.C., "NATO C^3I Architectures - Objectives and Organization", pps. 16-19 in (AFCEA89).

(COV88) Coviello, G. et al., "US DOD Efforts Towards Standards and ISDN Planning", in (AFCEA88) pps. 40-44.

(COP90) "Copernicus Architecture", Copernicus Project Team, Space and Electronic Warfare (OP-094), Office of Chief of Naval Operations, US Navy, Washington DC, 1991.

(CUL87) Cullen, J.S., "Evolutionary Development of Command Control Information Systems (CCIS) in the United States" pps. 102-105, in (AFCEA87).

(CUL88) Cullen, J.S., "Interoperability, Evolutionary Acquisition and New Technology: A Challenge for NATO" pps. 131-136, in (AFCEA88).

(DAR87) Dart, S.A. et al. "Software Development Environments", IEEE Computer, Nov. 1987, pps. 18-28.

(DAY90) Day, A.M., Dorman, D.M.,"Towards an Australian Broadband Network Infrastructure", Telecomms. J. Aust, Vol. 40, No. 2, 1990, pps. 3-14.

(DCA86) "Command, Control, and Communications Technology Assessment : Conference Proceeedings", 17-19 November 1986, DCA, Washington, DC, 1986, pps I-6, I-7.

(DCA89) "Command, Control, and Communications Technology Assessment: Conference Report", 31 Jan- 1 Feb 1989, DCA and JDL, Washington, DC 1989, pps.2 and 8-9.

(DCC91) "Defence Communications Corporate Plan 1991-2001", Department of Defence, AGPS, Canberra, May 1991.

(DEE90) Deer, P.,"Broad Functional Requirements Study for HQADF", Report ERL-0518-RE, ERL, DSTO Salisbury, May 1990 (DRAFT) (RESTRICTED).

(DEP91) De Pompa, B.,"Open Systems Me", UNIX World, Feb 1991, pps. 49-52.

(DIE90) Diedrichsen, L.D.,"Lessons Learned from Two US Army Evolutionary Acquisition Projects", in (EPIS90), pps. 55-63.

(DII91) Di Iorio, N.,"Integrating ISDN and OSI: An Example", IEEE Network Magazine, Jan. 1991, pps.10-23.

(DOA87) "The Defence of Australia", White Paper, Dept. of Defence, Canberra, March 1987, pps. 60-62

(DOU90) Dougall,C.J.,"Broadband Network Evolution in Telecom Australia", IEEE Communications Magazine, April 1990, pps. 52-54.

REFERENCES (continued)

(DSB78) quoted in (MAY88), p. 53.

(EPIS90) Proceedings of Evolutionary Procurement of Information Systems Symposium, EPIS'90, The Hague, Netherlands 11-14 June 1990: NATO Shape Technical Centre.

(FRA89) Fraase, M.,"MacIntosh Hypermedia", Scott, Foresman and Co., Glenview, IL., US, 1989.

(FSR91) "Force Structure Review", Report to the Minister for Defence, Department of Defence, DPUBS 35/91, Canberra, ACT, May 1991.

(GAG87) Gagliardi, D.,"Pan-European ISDN: Standards and Development", in (AFCEA87), pps.45-48.

(GIO91) Giordano, F., Wong, B., McCollum, L., "Rapid Development Speeds Path for Command System", Signal, April 1991, pps. 52-56.

(GRA82) Gravely, S.L.,"The Ocean Surveillance Information System (OSIS)" Signal, Oct. 1982, pps. 30-36.

(GRE83) Green, C., Luckham, D., et al. "Report on a Knowledge-Based Software Assistant", Report KES.U.83.2, Kestrel Institute, Palo Alto, CA., June 15, 1983.

(HAN89) Handel, R., "Evolution of ISDN Towards Broadband ISDN", IEEE Network Magazine, Jan. 1990, pps. 7-13.

(HEN90) Henderson-Sellers, B., Edwards, S.M., "The Object-Oriented Life Cycle", Comms. ACM, Vol 33, No.9, Sept 1990, pps. 143-159.

(HEN91) Henderson, D.E., "Evolutionary Acquisition and Procurement of Command Support and Military Information Systems for the ADF", ERL-0565-RE Report, ERL,DSTO Salisbury, August 1991 (DRAFT) (RETRICTED).

(HOL87) Holmes,J.E., Morgan, P.D., "A Layered Approach to the Representation of Naval Command Systems", Proceedings of 2nd IEE International Conference on Advances in C3IT, Bournemouth, England, April 1987, pps. 26-30.

(HOL88) Holmes, J.E., Morgan, P.D., The Specification and Design of Implementable Systems", in (SCC88), pps 93-99.

(HOO91) Hood, S.,"Report on Visit to Alaska, May 1991", ITD, ERL, DSTO, Salisbury, September 1991 (UNCLASSIFIED).

(JAC91) Jacobson, I.,"Industrial Development of Software with an Object-oriented Technique", J. of Object Oriented Programming, March/April 1991, pps. 30-41.

(JON90) Jones, S.P., "Rapid Prototyping : For Want of Better Words" (U) ERL-0526-TR, ITD, ERL, DSTO Sept 1989.

(JOS91) Joseph, J.V. et al.,"Object-Oriented Databases: Design and Implementation", Proc.IEEE Vol.79, No.1, Jan. 1991, pps. 42-63.

(JSP8) "Joint Operations ; Command and Control of Australian Defence Force Operations", JSP(AS)8, Interim 4-th Edition, Dept. of Defence, Canberra, October 1988.

(JSP84) "Joint Services Staff Manual: Glossary", JSP(AS)101, 3-rd Ed., Dept. of Defence, Canberra, Feb. 1984.

REFERENCES (continued)

(KER88) Kerr, I.E.,"The NATO C^3 Strategic Plan - A Means to Achieve Economic Integration of Emerging Technologies", pps. 127-131 in (AFCEA88).

(KOS88) Koschmann, T., Evens, M.w.,"Bridging the Gap between Object-Oriented and Logic Programming", IEEE Software, July 1988, pps. 36-42.

(KIN88) King, W.H., Ruoff, K.,"Command Level Decision Support Systems for NATO: Applications and Development Methodology", pps. 59-65 in (AFCEA88).

(LAT88) Lathouwers, G., Verhaegh, M.,"LAN versus ISDN for Data Services", in (AFCEA88), pps. 52-56.

(LEG89) Le Gall, p. et al., "Architectural Principles for French Military ISDN Signalling System", in (AFCEA89), pps. 42-46.

(LYO86) Lyons, R.E., "Conference Summary and Overview", pps.I-1 to I-31 in (DCA86).

(MAR90) Martin, J.,"Information Engineering", Books 1-3, Prentice-Hall, New Jersey, USA, 1990.

(MAR91) Marquess, P., "Object-Oriented Paradigm", DEC Professional, March 1991, pps. 50-59.

(MAY88) Mayk,I. and Rubin,I. "Paradigms for Understanding C^3, Anyone?" pps. 48-61, in (SCC88).

(MER86) Mercer, R.A., Edwards, W.L., "Issues in the Migration of Military Communications to an ISDN', IEEE MILCOM'86, pps. 50.5.1-5.

(MEY88) Meyer, B., "Object -Oriented Software Construction", Prentice-Hall, New York, 1988.

(MOR91) Orr, T.M., Morgan, G.A.,"Terrain Intelligence From Landsat TM : Katherine/Tindal RAAF Base, Northern Territory", Task ARM 86/100, Contractor Report No. 6, ITD, ERL, DSTO, Salisbury, Feb. 1991 (CONFIDENTIAL).

(OVE89) Overmyer, S.P., "Survey of Rapid Prototyping Tools for User-Computer Interface Design", CTC-TN-89-001, CONTEL Corp., Chantilly, VA. USA, Dec 13, 1989.

(POT87) Potts, J., "ISDN and Satellites", IEEE INFOCOM'87, pps. 359-360.

(REW89) Proceedings of "Requirements Engineering and Rapid Prototyping Workshop", US Army CECOM and TTCP XTP-2, Ft.Monmouth, NJ, 14-16 Nov 1989, pps. 23-26.

(RIC91) Richmond, K.,"Information Engineering Technology: A Method for Competitive Advantage", Telematics and Informatics, Vol.8, Nos. 1/2, 1991, pps. 41-57.

(RON90) Ronayne, J., "ISDN: Will the Future Ever Arrive?", Proceedings of International Conference "Network Directions", Birmingham,June 1990, (Blenheim Online, UK), pps 1-17.

(RUB88) Mayk, I., Rubin, I.,"Architectural Concepts for C3 Systems", Proceedings IEEE MILCOM'88, San Diego,CA., IEEE Press,NY, pps.16.2.1-16.2.7.

(SCC88) "Science of Command and Control Part I: Coping with Uncertainty", ed.Johnson, S.E.and Levis, A.H., AFCEA International Press, Washington, D.C. 1988.

(SCC89) "Science of Command and Control Part II: Coping with Complexity", ed. Johnson, S.E. and Levis, A.H., AFCEA International Press, Washington, D.C., 1989.

REFERENCES (continued)

(SCH89) Schone, C.L., "The NATO C^3 Goal Architecture - The NATO C3 System", in (AFCEA89), pps. 20-24.

(SHO90 Shore, D., "Evolutionary Development and Acquisition of C^3I Systems" pps.135-149 in (EPIS90).

(SMP90) "Software Strategic Plan", Office of Director (DR&E), US Department of Defense, Washington, DC, Feb. 1990. (Preliminary Draft). p. C-24.

(SOC87) Sochaczewski, J.M.,"NATO Information Systems in Support of Consultation and Military Command and Control", in (AFCEA87), pps. 73-77.

(SOR89) Sorenson, H.W., "A Discipline for Command and Control", in (SCC89), pps 7-11.

(STA90) Starr, S.H. and Alberts, D.S., "The Requirements Process for the Evolutionary Procurement of Information Systems", pps. 151-159 in (EPIS90) (Quote).

(STE88) Steer, D.G. et al. "Secure Communications with the Integrated Services Digital Network (ISDN)", in (AFCEA88), pps. 44-49.

(SWI91) Swift, M.K.,"Hypertext : A Tool for Knowledge Transfer", J. of Systems Management, June, 1991, pps. 35-37.

(THO87) Thompson, P.,"Reference Models for Information Engineering", First. Symp. Knowledge-Based Integrated Information Systems Engineering, Feb. 1987, MIT, Cambridge, MA..

(TOU88) Tournes, C., "*CUBE TOOL - A C^3I Specification-Oriented Tool*", pps. 24-30 in (AFCEA88).

(TAF90) Taffarello, R., " C^3I and Evolutionary Acquisition" , pps. 136-139 in (AFCEA88).

(USA90) Klose, R.R.,"ALBM ATTD Program", presentation at USA CECOM Center for C^3 Systems, Ft. Monmouth, NJ,Feb. 1990.

(UNI90) Kuhns, R.,"USAF Advanced Planning System (APS)", UNISYS presentation at TTCP STP-9 Meeting, NOSC, San Diego, CA, 24 July 1990.

(USJCS88) "US DOD Dictionary of Military Terms - JCS", Arco/Simon and Schuster, New York, NY 1988.

(VHO89) van Horn, J.H.,"A NATO ISDN Reference Architecture", in (AFCEA89) pps. 31-35.

(VTR89) van Trees, H.L., "C3 Systems Research : A Decade of Progress", in (SCC89), pps 24-44.

(WAL90) Waltz, E. and Llinas, J.,"Multisensor Data Fusion", Artech House, Boston, MA.,1990 (in particular references at end of chapter 5).

(WEI83) Weik, M.H.,"Communications Standard Dictionary", Van Nostrand Reinhold Co., New York, 1983.

(WEL89) Wells, E.J., "Management and Control of the NATO ISDN (NISDN)", in (AFCEA89), pps. 36-41.

(WID88) Widdicks, J.A., "Concept for a NATO ISDN", in (AFCEA88), pps. 49-52.

REFERENCES (continued)

(WIL91) Williams,R.J.,"Seminar/Workshop on GIS and Automated Cartography", 13-16 May, 1991, Army Survey Regiment, Royal Australian Army Corps, Bendigo, VIC.

DISTRIBUTION

	Copy No
Defence Science and Technology Organisation	
Chief Defence Scientist	)
Central Office Executive	) 1
Counsellor, Defence Science, London	Cnt Sht *
Counsellor, Defence Science, Washington	Cnt Sht *
Scientific Adviser, Defence Central	2
Scientific Adviser to Director Defence Intelligence Organisation	3
Naval Scientific Adviser	4
Air Force Scientific Adviser	5
Scientific Adviser, Army	6
HQADF	
VCDF	7
ACOPS	8
DGCCC (for DCSS)	9
Commandant, ADF Warfare Centre Attn: DD	10
ACDEV	11
DGCIS	12
DGFD (Sea)	13
DGFD (Air)	14
DGFD (Land)	15
Electronics Research Laboratory	
Director	16
Chief Information Technology Division	17
Chief Communications Division	18
Chief Electronic Warfare Division	19
Chief Guided Weapons Division	20
Special Adviser to CITD	21
Research Leader Command and Control	22
Research Leader Intelligence	23
Research Leader Combat Systems	24
Head Command Support Systems Group	25
Head Information Systems Development Group	26
Head Information Processing and Fusion Group	27
Head Software Engineering Group	28
Head Trusted Computer Systems Group	29
Head Architectures Group	30
Head VLSI Group	31
Head Image Information Group	32
Head Combat Systems Integration Group	33
Head Tactical Command Information Systems Group	34
Head Exercise Analysis Group	35
Head Combat Systems Technology Group	36
Head Combat Systems Effectiveness Group	37
Publications and Component Support Officer	38
Graphics and Documentation Support	39
Air Office	
ACAUST	40
DCIS-AF	41
DGMAT-AF	42
Navy Office	
MCAUST	43
DNC&I	44

DSSI	45
Army Office	
LCAUST	46
DCIS-A	47
Commandant, EDE	
Attn: CE and SSE Div	48
DIO	
DIDS	49
A&LO	
ASCOMMP	50
DJPR	51
Libraries and Information Services	
Australian Government Publishing Service	52
OIC, Technical Reports Centre, Defence Central Library Campbell Park	53
Manager, Document Exchange Centre, Defence Information Services	54
National Technical Information Service, United States	55-56
Defence Research Information Centre, United Kingdom	57-58
Director Scientific Information Services, Canada	59
Ministry of Defence, New Zealand	60
National Library of Australia	61
Defence Science and Technology Organisation Salisbury, Main Library	62-63
Librarian Defence Signals Directorate, Melbourne	64
British Library Document Supply Centre	65
TTCP	
CNL STP-9	66
UKNL STP-9	67
USNL STP-9	68
US Army Member STP-9	69
US Navy Member STP-9	70
Universities	
George Mason University, Centre for Excellence in C^3I, Fairfax, Virginia, USA	71
Spares	
Defence Science and Technology Organisation Salisbury, Main Library	72-77

Department of Defence

DOCUMENT CONTROL DATA SHEET

Page Classification	UNCLASSIFIED
Privacy Marking/Caveat	N/A

1a. AR Number AR-006-775	1b. Establishment Number ERL-0573-RE	2. Document Date FEBRUARY 1992	3. Task Number

4. Title

TOWARDS A C^3I STRATEGIC PLAN
PHASE 1: PRELIMINARY CONSIDERATIONS

5. Security Classification

Document	Title	Abstract
U	U	U

S (Secret) C (Confi) R (Rest) U (Unclass)

- For UNCLASSIFIED docs with a secondary distribution LIMITATION, use (L) in document box.

6. No. of Pages	108
7. No. of Refs.	96

8. Author(s)

Victor C. Sobolewski

9. Downgrading/Delimiting Instructions

N/A

10a. Corporate Author and Address

Electronics Research Laboratory
PO Box 1600
SALISBURY SA 5108

10b. Task Sponsor

11. Officer/Position responsible for

Security.......................SOERL.......................

Downgrading.......................DERL.......................

Approval for Release........DERL.......................

12. Secondary Distribution of this Document

APPROVED FOR PUBLIC RELEASE

Any enquiries outside stated limitations should be referred through DSTIC, Defence Information Services, Department of Defence, Anzac Park West, Canberra, ACT 2600.

13a. Deliberate Announcement

No limitation

13b. Casual Announcement (for citation in other documents)

☑ No Limitation

□ Ref. by Author , Doc No. and date only.

14. DEFTEST Descriptors

Australian Defence Force, Strategic planning, Command control communications and intelligence, Command control communications and intelligence systems.

15. DISCAT Subject Codes

2505, 1506

16. Abstract

The 1987 Defence White Paper highlights important developments, either put in place or foreshadowed, relating to .he ADF's capabilities in Command, Control, Communications and Intelligence (C^3I). The more recent Defence Strategic Planning and Force Structure Review stress the key role of C^3I in underpinning the principal roles of Defence and of the ADF.

A Strategic Plan for C^3I is required to manage the development and acquisition of future and long-term ADF C^3I requirements in a consistent, coordinated and effective way. Such a Strategic Plan will need to : identify the objectives for C^3I as well as the resources required to achieve these; specify a C^3I goal architecture; and propose a road map or "Migration Plan" to transition from the ADF's existing or currently proposed C^3I systems to the envisioned state-of-the-art C^3I systems.

This Initial Report considers the basic problems associated with C^3I development; reviews technologies, tools and methods to support this; and makes recommendations which form the first phase of a C^3I Migration Plan.

16. Abstract (CONT.)

17. Imprint

Electronics Research Laboratory
PO Box 1600
SALISBURY SA 5108

18. Document Series and Number	19. Cost Code	20. Type of Report and Period Covered
RL-0573-RE	822522	REPORT

21. Computer Programs Used

N/A

22. Establishment File Reference(s)

N/A

23. Additional information (if required)