COMMAND & CONTROL AS AN OPERATIONAL FUNCTION OF INFORMATION WARFARE IN THE CONTEXT OF "INFORMATION" – THE NATURE OF INFORMATION AND INFORMATION TRANSFER

Raymond J. Curts, Ph.D., (CDR, USN Ret.)
Strategic Consulting, Inc.
Fairfax Station, Virginia
rcurts@ispwest.com
(703) 731-0301 (cell)

Douglas E. Campbell, Ph.D., (LCDR, USNR-R, Ret.)
Syneca Research Group, Inc.
Washington, D.C.
dcamp@syneca.com
(703) 627-4257 (cell)

2004 Command and Control
Research and Technology Symposium

15 – 17 June 2004
San Diego, CA

COMMAND & CONTROL AS AN OPERATIONAL FUNCTION OF INFORMATION WARFARE IN THE CONTEXT OF "INFORMATION" – THE NATURE OF INFORMATION AND INFORMATION TRANSFER

Raymond J. Curts, Ph.D., (CDR, USN Ret.)*
Strategic Consulting, Inc.
Fairfax Station, Virginia
rcurts@ispwest.com
(703) 731-0301 (cell)

Douglas E. Campbell, Ph.D., (LCDR, USNR-R, Ret.)
Syneca Research Group, Inc.
Washington, D.C.
dcamp@syneca.com
(703) 627-4257 (cell)

* Point of Contact

ABSTRACT

There are established characteristics that bound the conduct of Information Operations (IO), Command and Control (C^2) and Net-centric Warfare within the Department of Defense (DoD). These characteristics specifically describe the intended information infrastructure as installed aboard aircraft, ships, submarines and other warfare assets, in training facilities, at shore-based sites and deployed with forward units. Over the past few years, military posturing has changed from focusing on static superpower confrontations to regional conflicts involving dynamic alliances. This has naturally led to the need for new military strategies and tactics, which have, in turn, highlighted the need for "information superiority." At issue is that Information Warfare has taken on a new meaning. The consequences of recent wartime events have led to the need for an integrated information capability that not only meets the needs of command and control in today's modern warfare tactics but which also can be provided in an affordable and near-term manner.

Deleted: 26

1.0 INTRODUCTION

Information Operations (IO), with all of its many divisions and evolutions, is a mission area including the operational functions of Command & Control (C^2). To achieve information superiority, IO must be capable of making use of the underlying command, control and communications architectural infrastructure in all operational stages from concept through planning, modeling & simulation to execution in an actual operational environment. Information systems designed to aid in decision-making are commonplace in C^2 operations and the ability to build, operate and maintain IO systems is crucial to the effectiveness of C^2. The authors' argument is that we need the ability to establish a solid information infrastructure for C^2 decision-making based upon rigorous, standardized architecture definition, development, analysis, description and acquisition planning.

With significant investments and "lessons learned" already made by the Department of Defense in IO, Information Warfare (IW), Command & Control Warfare (C^2W) and C^2, the intent of this paper is to highlight the steps necessary to proceed in an incremental and evolutionary acquisition manner; to define the long-term vision; and then to delineate achievable increments such that the sum of the increments will implement the goal. To this end, the authors' approach will be to lay out a series of basic concepts that should serve as blueprints for evolutionary development and then to define and expand upon two specific documents: the Integrated IW Master Plan [IWMP, 1996] and the IW Implementation Plan [IWIP, 1996] which deal with the programmatics of evolutionary acquisition.

Information has become widely recognized as critical to the success of modern warfare. As a backdrop for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C^4ISR) efforts, Information Warfare (IW) can be defined as that set of functions designed to achieve information superiority in support of national military strategy by effecting adversary information and information systems while leveraging and protecting our own information and information systems. The intent of this paper is to clearly delineate, describe and understand the boundaries of IO, IW and C^2; establish a basis from which an integrated information infrastructure can be developed; and allow the formulation of basic programmatic strategies.

> *"**Industrialization** led to attritional warfare by massive armies. **Mechanization** led to maneuver predominated by tanks. **The information revolution** implies the rise of cyberwar, in which neither mass nor mobility will decide outcomes; instead, the side that knows more, that can disperse the fog of war yet enshroud an adversary in it, will enjoy decisive advantages."*
>
> --John Arquilla and David Ronfelt, RAND

> *"Machines don't fight wars. Terrain doesn't fight wars. Humans fight wars. You must get into the mind of humans. That's where the battles are won."*
>
> --COL John Boyd, USAF

Deleted: 26

2.0 BACKGROUND

The research for this paper began in the early-1990s when the newly-formed Information Warfare Directorate (PD16) of the Space and Naval Warfare Systems Command (SPAWAR) needed an Information Warfare Master Plan (IWMP), an Implementation Plan and an Acquisition Strategy. The intent of such documents was to capture the necessary and sufficient information required to construct an architecture upon which to build implementation programs. To do so required the authors to define and bound the geographic expanse of IO / IW, the platforms and other entities that are involved in the context of "information" and then define and bound the nature and mechanism of the interactions (i.e., the nature of information and the information transfer). Since that time the authors have continuously perused, studied and integrated the functional capabilities associated with all areas of IO across a number of initiatives. The authors work in the areas of information architectures, interoperability and information assurance on a daily basis and are constantly reviewing the latest published studies and reports, supporting infrastructure and the functions and characteristics of the subsystems and segments incorporated within the overall system. There have been a very large number of architecture, interoperability and information assurance studies, projects, programs and other initiatives since the authors began to keep track in the late 1980s. To date, none has lasted long enough to produce repeatable, quantifiable, results that can be used consistently and repeatedly to impact acquisition. Hence, a glaring shortfall across all such initiatives appears to be the matter of sustainability. These issues will also be discussed in this paper.

2.1 <u>The IW Vision</u>

The quest for information dominance will decide the outcome of future warfare. Control of information that is both global in scope and focused on the battlespace will be a critical feature of all military operations. Advanced, strategically located IO / IW / C^{2}W / C^{4}I systems will assemble, integrate, and disseminate the information needed by users at all levels. An absolutely coherent, accurate, fully-integrated, all-source, timely picture of the total battlespace will be a force multiplier and will provide Combatant Commanders with the world's premier, forward deployed IO / IW / C^{2}W / C^{4}I capability. Similarly, an accurate, fully-integrated, all-source, targeting-quality picture will provide "shooters" with tactical superiority.

The vision for Information Operations, both Information Warfare and Operations Other Than War (OOTW), can be simply stated as, "Information Superiority through the availability and use of the right information, at the right place, at the right time, to all decision makers, while denying that information to the enemy." At the conceptual level, "IW consists of all efforts to control, exploit, or deny an adversary's capability to collect, process, store, display, and distribute information, while at the same time preventing the enemy from doing the same." [Garigue, 1995] Within the Department of Defense (DoD) IW is a fully integrated, embedded, joint, interoperable core set of functional modules building upon the infrastructure and technical capabilities of existing systems augmented as necessary with new / enhanced functionality provided by advanced technologies that fully satisfy validated operational requirements providing a forward deployed, Joint IO capability.

Deleted: 26

"Our present theory is to destroy personnel, our new theory should be to destroy command. Not after the enemy's personnel has been disorganized, but before it has been attacked, so that it may be found in a state of disorganization when attacked."

-Extracted from J.F.C. Fuller, Memorandum
"Strategic Paralysis as the object of the Decisive Attack", May 1918.

3.0 CONSIDERATIONS

As articulated by the Chief of Naval Operations and the Commandant of the Marine Corp in their memorandum of February, 1995 [CMC, 1995], there are many disparate disciplines being brought together under the umbrella of IW / C^2W. Since the early stages of IW / C^2W development, the process of defining, designing, developing, procuring and managing IW / C^2W / C^4I systems has been very narrowly focused, as well as, program and threat specific. In order to be effective, we must leverage existing, "legacy" capabilities wherever applicable to meet future requirements. We must integrate select legacy systems while providing the growth area needed to effectively implement advanced capabilities as they become available. Any IW architecture must integrate the full life cycle considerations of exploit, protect, and attack capabilities while ensuring information can be shared rapidly, efficiently, routinely and jointly by the commanders who work the joint battle fields of the future.

3.1 <u>Organizational Considerations</u>

IO capabilities and systems are procured and supported by a large variety of diverse organizations with little or no coordination of effort, consolidation of functional capabilities, nor concern for interoperability issues. The major hardware and software providers ("prime" contractors) are generally the most (and possibly the only) technologically knowledgeable participants in the design, development, procurement process. For the most part, there is no clear description of where and how systems interface with each other or the world around them and, in many cases, no "honest broker" to ensure adherence to architectural concepts. One exception may be the Global Information Grid (GIG), where the Defense Information Systems Agency (DISA) could be considered its "honest broker". The GIG is being architected as a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

The GIG is planned to include all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG is intended to support all Department of Defense (DoD), National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG is planned to provide capabilities from all operating locations (bases, posts,

Deleted: 26

camps, stations, facilities, mobile platforms, and deployed sites) and to provide interfaces to coalition, allied, and non-DoD users and systems. [DISA, 2004]

Back in 1993, the Defense Science Board (DSB) Task Force on Information Architecture for the Battlefield concluded,

> *"Information Warfare is a national, strategic concern. Our economy, national life and military capabilities are very dependent upon information - information often vulnerable to exploitation or disruption."*
>
> [DSBIAB, 1994]

At about the same time the Defense Science Board (DSB) twice commented that DoD needs a highly placed C^4I Architect and "... a coordinated DoD approach with standardized guidelines that would be applicable to all Services." [DSBGS, 1993] and [DSBR, 1994]. Clearly, this concept applies to IO at all levels from the President to the warfighter.

3.2 <u>Operational Considerations</u>

Effective, integrated strategic Information Operations and Command and Control (IO / C^2) capabilities provide the National Command Authority (NCA) a leveraged position against an adversary prior to the advent of traditional hostilities. In tactical applications, it gives the commander an enhanced capability to readily observe, orient, decide and act while slowing or negating that same process for the adversary. Effective IO / C^2W require dedicated and focused intelligence support and must be fully integrated with the C^4I infrastructure. The information infrastructure must support the IO / C^2W / C^4I missions from inception. Threat analysis, C^2 nodal analysis, digitized charts, imagery, HUMINT, SIGINT, navigation, and open, clear, and protected communications must be available. It is critical that planners determine what granularity of product will be required by each respective level of the warfighting team. Delivery of the required level of granularity is a key element of effective information warfare.

The perishable nature of capabilities, both ours and those of our adversary, dictate levels of sensitivity associated with certain information. Certain IO / C^2 capabilities will require greater degrees of protection than others. For these programs, the key to operational success will be the integration of operators into the planning and development stages early-on to ensure effective integration of the capability into the operational forces. These more sensitive capabilities may be protected within special access programs.

IW, the segment of IO dealing with conflict, provides enhanced capability in the areas of mission planning and preparation, C^4I support, analysis, information security and attack. As defined by the Roles and Missions Commission IW includes, "Offensive and defensive measures aimed at controlling, disrupting, or destroying an adversary's information flow while protecting one' own." [RMC, 1995] Specifically, the functionality of IW includes the areas of IW Protect, IW Exploit and IW Attack.

Deleted: 26

4.0 FUNCTIONAL RELATIONSHIPS

Information Warfare functional capabilities fall into three basic functional areas: Protect, Exploit and Attack. Within these broad areas there are five pillars of Command & Control Warfare (C^2W) which can be thought of as a natural subset of IW with specific application to C^2. These pillars embody the essence of C^2W capabilities: Military Deception (MILDEC), Psychological Warfare (PSYOPS), Operational Security (OPSEC), Electronic Warfare (EW) and Physical Destruction (Attack). Although we do not find these terms used as broadly today as they once were, the basic concepts still apply, some to more than one broad area of IW.

The military application of Information Warfare, Command and Control Warfare, or Command, Control, Communications, Computers and Intelligence (C^4I) is an element of military strategy that employs the full range of naval, joint, coalition and national means--both lethal and non-lethal--to attack our adversary's ability to command and control his forces while simultaneously protecting our own command and control. It is an approach to warfare that supports military operations at all levels of conflict, including those prior to hostilities. To realize the full potential of C^2W, the commander must integrate all five pillars of C^2W. Successful C^2W depends upon the synergy achieved by coordinating the application of each element. An essential factor in executing each of the elements of C^2W the C^4I systems is the supporting infrastructure. The C^4I system leverages our advantages in technology and encompasses surveillance, communications, and information management resources. [NDP 6] Figure 1 depicts the relationship between IO (its two main divisions: IW and OOTW), C^2W and C^4ISR in simplified form. The following paragraphs briefly discuss the individual pieces.

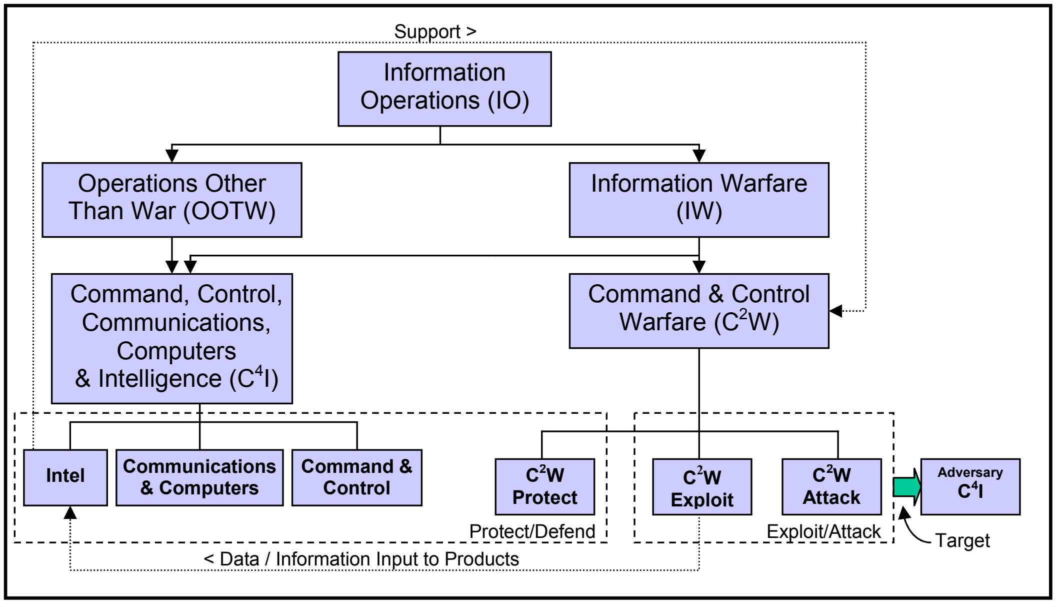
Support >
Information Operations (IO)
Operations Other Than War (OOTW)
Information Warfare (IW)
Command, Control, Communications, Computers & Intelligence (C4I)
Command & Control Warfare (C2W)
Intel
Communications & Computers
Command & Control
C2W Protect
C2W Exploit
C2W Attack
Adversary C4I
Protect/Defend
Exploit/Attack
Target
< Data / Information Input to Products

Figure 1: IO / IW / C^2W / C^4ISR Functional Relationships

Deleted: 26

4.1 Command, Control, Communications, Computers & Intelligence (C^4I)

C^4I can be decomposed in any number of ways. But, for our purposes we will discuss C^4I in three discrete segments: Command and Control; Communications and Computers; and Intelligence.

JCS Publication 1-02 defines C^4I as: The integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support the commander's exercise of C^2 through all phases of the operational continuum. [JP 1-02]

4.1.1 Command and Control (C^2)

C^2 can be defined as the actual process of directing and controlling forces. A generic Command and Control process is depicted in Figure 2 below [IWIP, 1996].

As defined in JCS Pub 1-02, C^2 is the exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. Command and Control is 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. (Extracted from JCS Pub 1-02)

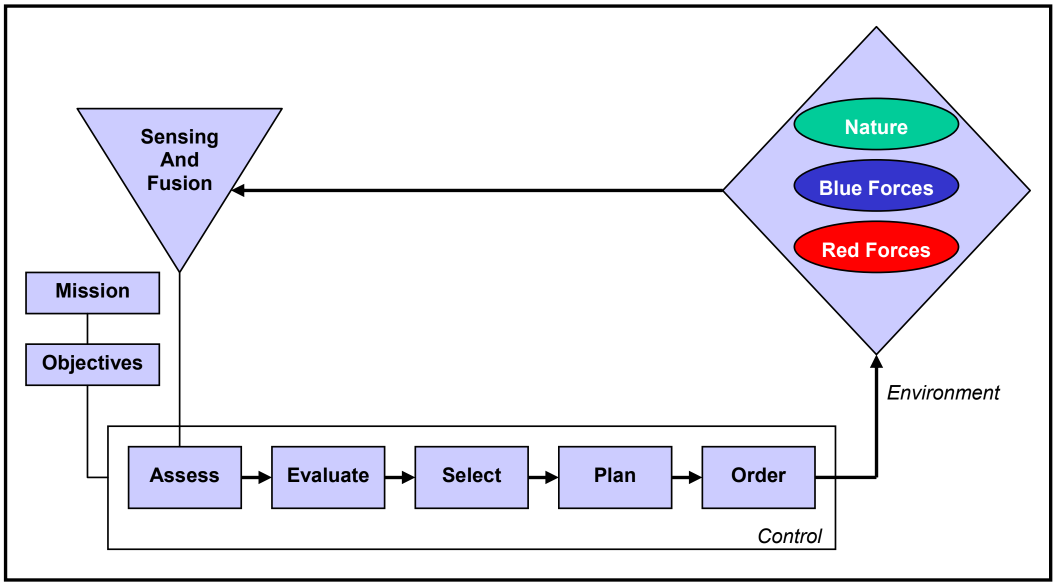

Figure 2: Command & Control (C^2) Process.

Deleted: 26

4.1.2 Communications and Computers

Communications and Computers are the facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the mission assigned.

> *"Communications dominate war; they are the most important single element in strategy."*
>
> Mahan (1907)

This piece can be thought of as the communications facilities, equipment, personnel, and procedures that provide the capability to process information, develop information, record information, and transfer information among participants in support of a military mission. The required attributes for communications and computers are speed, reliability, and security of information during processing and transmission. Operation of the Department's information systems relies on the computer and communications infrastructure which will enable operational and functional staffs to access, share, and exchange information worldwide with minimal knowledge of communications and computing technologies.

4.1.3 Intelligence

Intelligence is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; and information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding [JP 1-02].

Integrated intelligence and counterintelligence support are critical to C^2W as in every warfare area. This support requires the fusion of intelligence from a very large number and variety of disparate sources and is dependent upon interagency communication and cooperation. Planning, execution, and evaluation of both counter-C^2 and C^2-protection are necessary by commanders at all echelons from the inception of plans through implementation and evaluation. Precise intelligence is essential for operational planning and execution of C^2W; the operational commander must have the best available intelligence on enemy situations, intentions, and capabilities. Only with this information can the commander weigh the potential advantage of specific actions, assess the potential loss of intelligence from exploitation, and weigh the need to employ counterintelligence to protect intelligence sources and methods against the benefits of disrupting or destroying enemy C^2. [MOP 30]

There are four main categories of intelligence sources, also known as collection disciplines [CIA, 1993]. These categories are defined as follows:

1. **Signals Intelligence**, also known as SIGINT, which includes information derived from intercepted communications, radar, and telemetry and is the responsibility of the National Security Agency (NSA).

Deleted: 26

2. **Imagery**, referred to as IMINT, which includes both overload and ground imagery. The National Geospatial-Intelligence Agency (NGA) is responsible for the management of national and tactical reconnaissance requirements

3. **Measurement and Signature Intelligence** (MASINT) is technically derived intelligence data other than imagery and SIGINT and is handled by the Central MASINT Office within the Defense Intelligence Agency. The data result in intelligence that locates, identifies, or describes distinctive characteristics of targets.

4. **Human** source **Intelligence** (HUMINT) involves clandestine and overt collection techniques used mainly by CIA and the Departments of State and Defense.

4.2 Information Warfare Capabilities

Simply stated, information warfare seeks to obtain information dominance. Its scope includes both offensive and defensive operations. Nearly every Service and Agency has attempted to define IW for their own purposes and, while similar, few are the same. The National Defense University has devised a working definition for information warfare that we shall adopt:

> *"Information-based Warfare is an approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage especially in the joint and combined environment. Information-based Warfare is both offensive and defensive in nature—ranging from measures that prohibit the enemy from exploiting information to corresponding measures to assure the integrity, availability, and interoperability of friendly information assets. While ultimately military in nature, Information-based Warfare is also waged in political, economic, and social arenas and is applicable over the entire national security continuum from peace to war and from 'tooth to tail.' Finally, Information-based Warfare focuses on the command and control needs of the commander by employing state-of-the-art information technology such as synthetic environments to dominate the battlefield."*
>
> Hutcherson (1994)

As previously mentioned, IW was originally divided into Offensive and Defensive IW and / or IW Protect, Exploit and Attack. Although this terminology is not as readily apparent today as it once was, the categorization is still valid.

4.2.1 Information Warfare Protect Capabilities

Information Warfare Protect (IWP) includes all functions designed to protect friendly IW / C^{2}W / C^{4}I systems from unwanted interference. IWP can be thought of as an umbrella under which all other IW functions operate. Protection must be designed into every IW / C^{2}W / C4^{2}I

Deleted: 26

system from the outset. In addition, overarching programs, systems, concepts, policies and procedures must be developed.

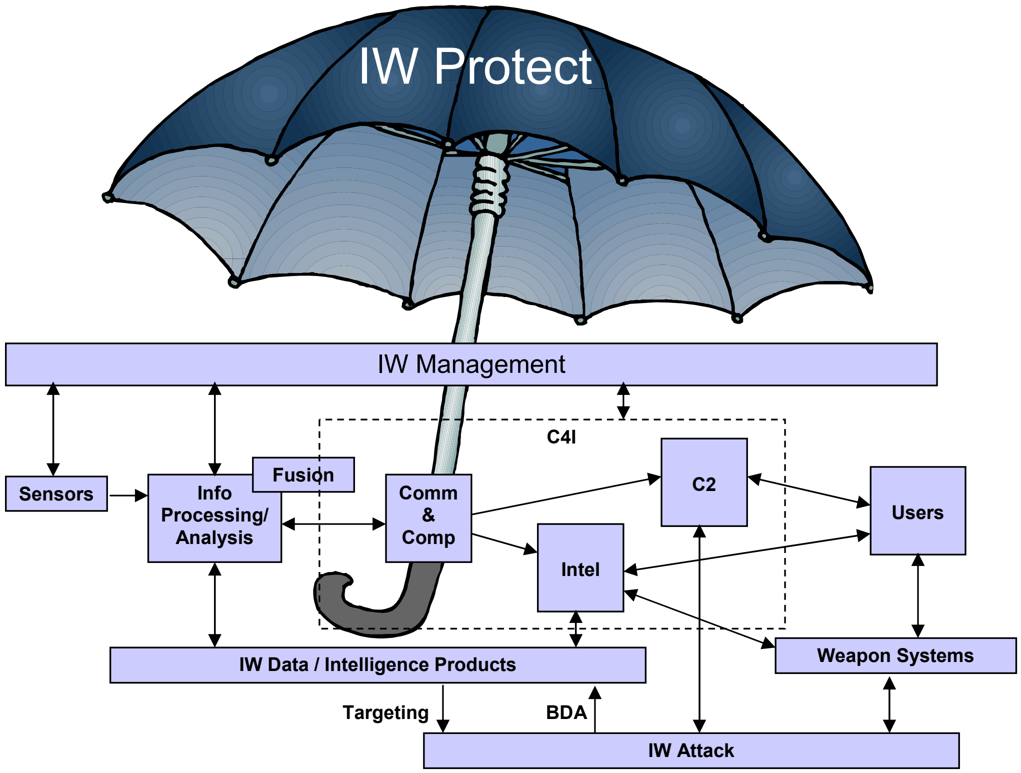

Figure 3: The Information Warfare Protect Umbrella

"Protect" measures must be considered in terms of life cycle, i.e., "cradle to grave". Admiral Owens once said that "…. we must make our systems impervious to an adversary." Within fiscal means, our vision is to make our C^4I systems as resistant as possible to any adversarial activities, and the involvement must begin while the system is on the drawing board. Then OSD/C3I's Information czar, Colonel Douglas Hotard, said it simply but eloquently when he addressed an Information Warfare symposium in December 1994:

> *"No commander should ever go to the battlefield relying on information that he cannot protect."*
>
> Hotard (1994)

Effective "protect" ensures that vulnerabilities of critical paths are assessed for essential systems. The problem set includes information systems, infrastructure, non-communications systems and weapons systems. They all use some combination of chips, software, computers, and transmission media. Essential legacy systems, regardless of life cycle stage, require

Deleted: 26

vulnerability assessments and appropriate remedial measures in order to ensure our effective use of information systems and information in attaining national objectives. Succinctly, legacy systems, by definition, are behind and we need to take a measured approach in elevating selected systems to an acceptable level in terms of risk management.

Computer Security, a subset of Information Assurance (IA), is concerned with the protection of the integrity, availability and, if needed, confidentiality of automated information and the resources used to enter, store, process and communicate it. Computer security is often referred to in conjunction with system trustworthiness, integrity, safety, availability and reliability. To effectively include computer security in the procurement process it must be integrated into the procurement cycle from its inception.

IWP is an area of information warfare intended to deny the enemy reasonable opportunity to attack and/or exploit our information resources. In order to be effective, protect measures must be pervasive (i.e., the weakest link is the most vulnerable, needs the most protection and defines the level of "Protection" for the entire enterprise). IWP measures must also address the entire life of the information. In order to do so, the requirements must be conceived concurrent with the system processing requirements and fully integrated into the acquisition life cycle.

Once operational, the protection measures must be sufficient to provide the requisite protection even while operating in severely reduced administration environments. Today's solutions will operate adequately in laboratories and under ideal administrative control. However, severe problems arise when such controls can not be adequately administer in a cost effective manner under all conditions.

Retirement of systems or information continues to be a life cycle problem which requires systemic measures. Sensitive information is placed on persistent media with extended life. In many cases this media life extends well beyond the life of the information itself. Mechanisms must be provided which permit the orderly release from protection of information which no longer needs such protection. This release is necessary if cost effective controls are to be placed on information actually requiring protection.

The means to advance the use of IWP are largely an acquisition issue. Incentives and requirements for providing such mechanisms within a system acquisition need definition. After definition, the current practice of using security requirements as tradeoff items must be stopped. Continuations of such practices increase the cost of protection for those systems which adhere to the standards, while perpetuating vulnerable links in our information environment.

4.2.2 Information Warfare Exploit Capabilities

Information Warfare Exploit (IWE) is concerned with exploiting the capabilities of our adversaries. IW Exploit includes all of the passive monitoring / analysis IW functions whereby targeted IW / C^2W / C^4I systems and associated infrastructures are exploited for the purpose of acquiring information.

Deleted: 26

Information Warfare Exploit (IWE) resides primarily within the C^{2}W area of Electronic Warfare (EW) under Electronic Support (ES). IWE / C^{2}W / EW / ES can be hosted in satellites, aircraft, ship borne, and land-based platforms. The IWE effort leverages our C^2 to gain higher performance levels than our adversary's through passive monitoring and related analysis functions whereby targeted systems and associated infrastructures are exploited for the purpose of acquiring information. The exploitation infrastructure and the associated skills are the most heavily developed of the IW disciplines. IWE synergistically feeds both IWP and IWA. In the context of C^{2}W, ES provides critical support to the other four C^{2}W elements. Two unique features of ES are that it provides real-time data and can provide direct insight into an adversary's intentions. The importance of the relationship to intelligence cannot be overstated. ES both feeds and receives cueing from the intelligence system. The advent of the Global Positioning System is a value added feature that, when used with passive monitoring and locating technology, allows our mobile platforms to precisely locate a target. We will constantly seek methods that facilitate executing C^{2}W Exploit on "non cooperative targets" and those that improve the IWE mission.

4.2.3 Information Warfare Attack Capabilities

Current Information Warfare Attack, or IWA, generally falls into three categories: hard-kill (e.g., High Speed Anti-Radiation Missile (HARM)), firm-kill (e.g., High Energy Radio Frequency (HERF) or Electromagnetic Pulse (EMP)) and soft-kill (e.g., jammers). As with many other existing IW systems, most are standalone, stove-piped legacy systems. The future of IWA should be one where the existing capabilities have been consolidated into an integrated, coordinated system capable of expanding the scope of IWA into more non-traditional areas (e.g., insertion of computer viruses into enemy systems).

IW Attack is considered to be any active interaction with a target IW / C^{2}W / C^{4}I system and/or infrastructure. IW Attack is any action taken to affect an adversary's information or information systems in a manner beneficial to U.S. interests. The execution of Attack can occur through the use of any capability within the DoD-wide arsenal of capabilities and may be an integrated process coordinated by the National Command Authority. It's important to recognize that technical information discovered in attack will often complement the IWP effort. IWA requires strong support from the intelligence community. Attack actions may be any active interaction with a target that disrupts, degrades, denies, negates, or destroys the target capability.

4.3 Command & Control Warfare (C^{2}W)

The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOPS), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the range of military operations and all levels of conflict. C^{2}W is both offensive and defensive:

a. Counter C^2: To prevent effective C^2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C^2 system.

b. C^2 Protection: To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade or destroy the friendly C^2 system. [Joint Pub 3-13]

Simply put, Command and Control Warfare is that portion of Information Warfare that is directly applicable to C^2 and C^2 systems.

5.0 IW ARCHITECTURE

We have stated that the goal should be a fully integrated, net-centric, global, enterprise capability that will enable a common awareness and promote shared understanding. This basically equates to Information Assurance which requires an interoperable infrastructure which, in turn must start with a well defined architecture. One of the first and most important pieces of an IW system is a well thought out, thorough, open, joint, interoperable IW architecture. This architecture begins as a high level concept, vision or strategy intended to serve as a "blueprint" for all IO systems, their interconnectivity and their connection to other services, organizations and agencies.

A standardized, well defined architectural process would significantly simplify the evolution of architectures while adding a certain amount of rigor, reproducibility, and confidence to the procedure. This process must, as a minimum, contained well defined authorities, designated cognizant activities, processes, milestones, architectural outlines and formats, deliverables, documentation and maintenance / upgrade schedules (see Figure 4).

Deleted: 26

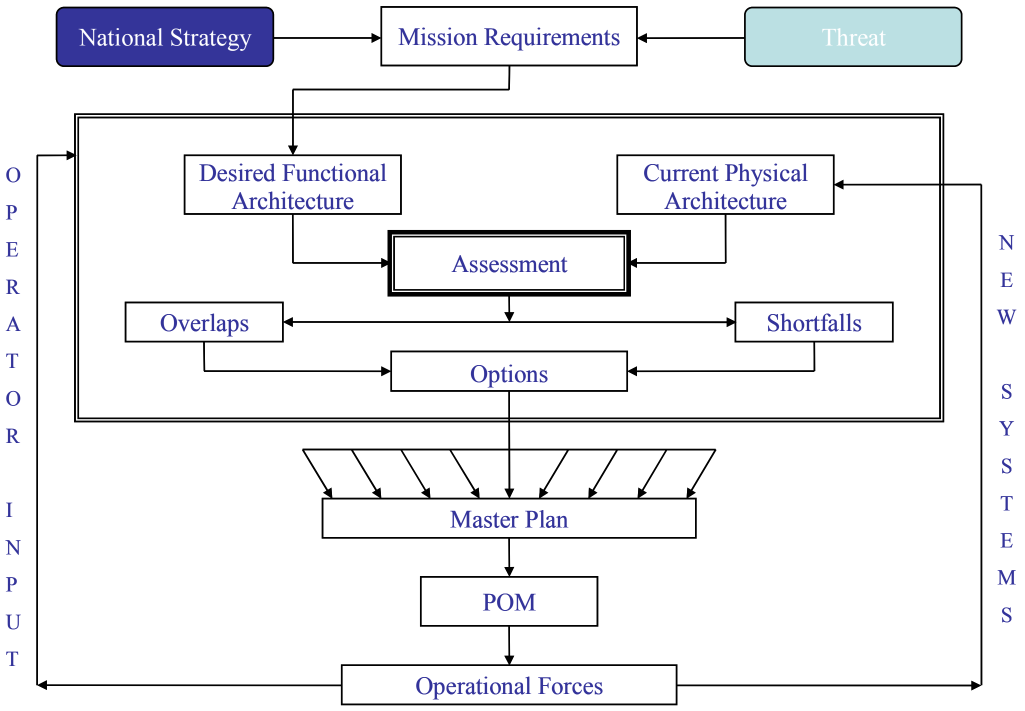

Figure 4: Information Architecture Process

5.1 IW Data Management

Information warfare data will need to be managed such that it is developed, installed, and evaluated within an operational system that basically allows commanders to design their own information warfare system or a conveniently grouped set of services. The data then needs to be delivered to warfighters as an accurate, timely, and consistent picture of the Joint / Coalition battlefield. The data will provide access to key transmission mechanisms and will most probably reside in worldwide data repositories. To achieve this goal, data will need to be managed such that it can exist in a system that will:

- expand the bandwidth by 100 to 1000 times for multimedia information delivery down to lower, mobile echelons (e.g., battalion);
- provide smart push and warrior pull via an information dissemination server (IDS) accessing multiple data sources to include national and theater intelligence, operational, and logistics information;
- provide information management technology to augment the various services and tactical networks to include data transport services (error recovery, levels of service, instrumentation, and diagnostics), information security, integrated database query and retrieval (repository mediation, information brokering, filtering, profiling, storage management, and data linking), and tools for commanders to enforce an information policy;

Deleted: 26

- use the data accessed via the IDS to create a graphical depiction of the current situation which is consistent across Services and up and down echelon within each Service and which is linked to a variety of supporting information;
- allow the user to tailor his view of the battlespace by drilling down through the supporting information infrastructure to display and manipulate the underlying data using a provided toolkit compatible with the various services and tactical network environments;
- provide the necessary hardware and software to be added to warfighter workstations to allow them to receive, request, store, manipulate, and view integrated information distributed by the various services and tactical networks;
- provide a capability which minimizes life cycle cost (e.g., maximize the level of automation since human operators are expensive resources); and
- deliver a system which contains the safeguards necessary to operate in an active information warfare environment.

To achieve these objectives, five system segments, each based on existing products and prototypes, will need to be integrated for data flow: the IDS; user applications software and equipment; a wideband, low-cost broadcast mechanism (GBS or equivalent); a means for the warfighter to request specific information from the field using existing communications (e.g., Joint Tactical Internet or Global Information Grid (GiG)); and the information sources and archives that the IDS accesses. The IDS stores data received from information sources including UAV and national imagery, operational data, and fusion and exploitation sources. The applications software will interface with existing tactical workstations and have the necessary receive equipment, software, and hardware to filter and store broadcast data and then present it as a fused picture of enemy and friendly forces integrated with terrain, image, and video data. Dissemination throughout the battlefield will be accomplished inexpensively using a GBS system derived from commercial direct digital broadcast satellite technology. The Joint Tactical Internet or GiG will be created by integrating standard commercial network protocols and services on top of existing tactical communications systems. Warfighters will be able to request needed information and then receive it via direct broadcast.

Building secure, interoperable information systems can be viewed from an engineering perspective as being very similar to constructing a car, a bridge, a building, an engine, or any major physical entity. They usually start with a complete, complex, well thought-out design / plan / blueprint / architecture. And these start out with data.

Even renovations of existing entities (cars, bridges, buildings, machinery, etc.) start with a description of what is there now and how it will be modified – i.e., from data comes a plan.

Well designed plans (Architectures) allow us to field fully connected, interoperable systems which then transport the required information to the decision makers (see Figure 5).

Deleted: 26

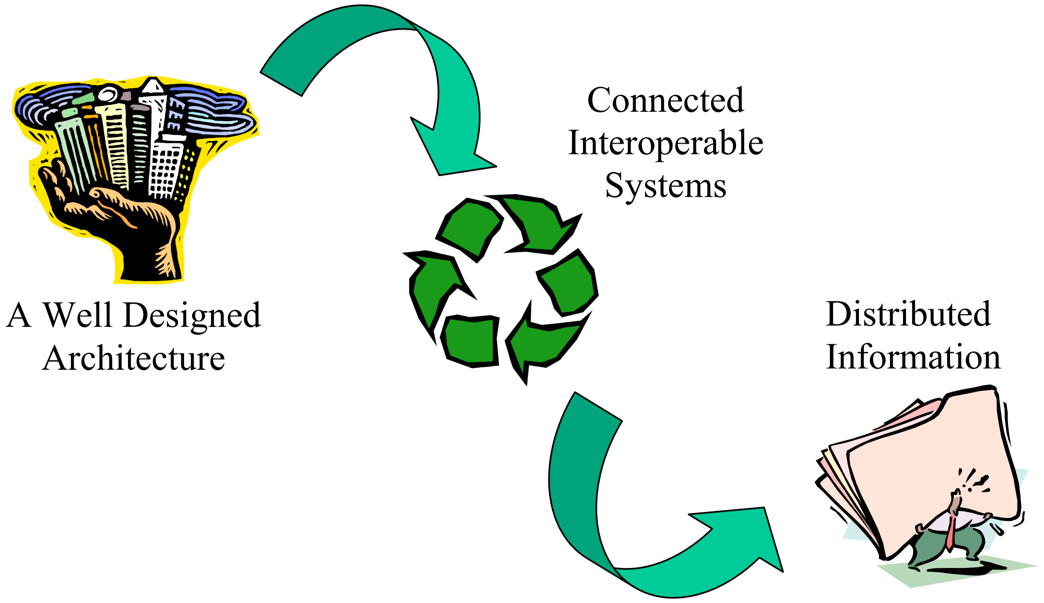

Figure 5: Information Flow to the Decision-Makers

5.2 IW Standards

We must define architecture development, definition, maintenance and interface standards as necessary (Figure 6) to:

- ENSURE interoperability and connectivity of architectures, consistency, compliance with applicable directives, and architectural information dissemination;

- FACILITATE implementation of policies and procedures, acquisition strategies, systems engineering, configuration management, and technical standards; and,

- STANDARDIZE terms of reference, modeling tools, architecture data elements, architecture data structures, hardware and software interfaces, architectural representations and architectural scope, and level of detail / abstraction.

The goal should not be forced procurement of a single, standard system that performs some specific set of functions. The real issue, at least in the near term, is not "Who is using what system?" but rather "Are these various systems compatible / interoperable?" In other words, all that is really needed, at least to start, is interface / interoperability standards.

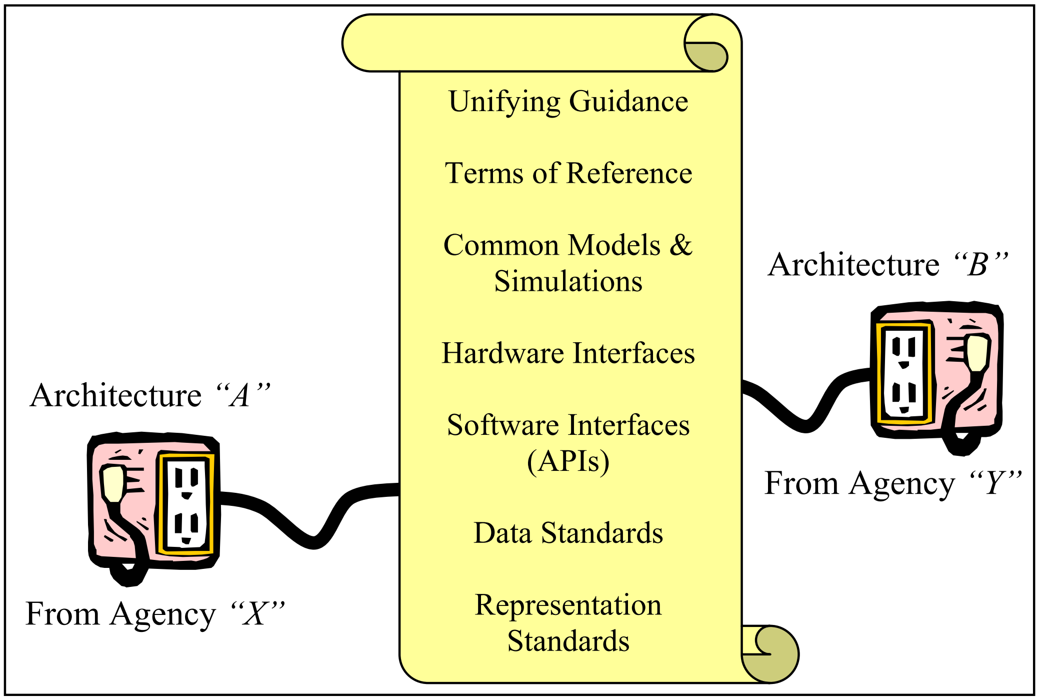

Figure 6: Interface Standards

6.0 SUMMARY

In summary, we look upon three of the most important aspects of Information Operations – data, management and process. IO data must become a distributed system of databases containing all data needed to support user requirements. IO systems must be able to access any data relevant to the products they are developing. All IO databases must be implemented using standard data structures. All IO databases need to be readily accessible by any processing/fusion system. Some of this work is already underway within the GiG Enterprise Services environment. Service Oriented Architectures (SoAs) seem to be the current direction to solve this problem. However, there are a number of other technologies / methodologies that may be useful including: Event Driven Architectures (EDA), Effects Based Operations (EDO) and others. While existing technology can and should be utilized to maximum effect, we must be careful not to commit too hard to any given solution before we run through the architecture process a few times such that we fully understand the problem.

IW Management must be a modular, distributed, networked system which monitors, controls, coordinates and optimizes IW support to the users. It must also provide the interfaces between IW / C^{2}W / C^{4}I. Modules must be located at all surveillance information processing / fusion nodes. Functional capabilities of each module must be matched to the level of its node. All modules need to be networked together via the information infrastructure. The system must ensure that products meet user needs. What will be required is a full push / pull architecture.

Deleted: 26

That is, a full worldwide network of modules. There will need to be close coordination with "owners" of sensors/data to ensure that user requests are rapidly assessed and responded to when needed.

And finally, the process must be well-defined, defendable, repeatable, and robust. The process must constantly evolve, with each iteration reducing risk and producing ever increasing accuracy and defendability. And, possibly most important of all, it must withstand the test of time. The process must be permitted to evolve through multiple iterations, possibly using evolutionary acquisition and spiral development strategies.

The publication of Department of Defense (DoD) Directive 5000.1 and DoD 5000.2 established a preference for the use of evolutionary acquisition strategies relying on a spiral development process. Evolutionary acquisition and spiral development are methods that allow a reduction in cycle time and speeds the delivery of advanced capability to the warfighter. These approaches are designed to develop and field demonstrated technologies for both hardware and software in manageable pieces. Evolutionary acquisition and spiral development also allow insertion of new technologies and capabilities over time. These approaches provide the best means of getting advanced technologies to the warfighter quickly while providing for continual improvements in capability. Evolutionary acquisition and spiral development are similar to pre-planned product improvement but are focused on providing the warfighter with an initial capability that may be less than the full requirement as a trade-off for earlier delivery, agility, affordability, and risk reduction. [DODD, 2003; DODI, 2003]

7.0 FUTURE INITIATIVES

Future initiatives in Information Warfare fall into four basic areas. The first area includes organizational, administrative or managerial initiatives. The second is programmatics or acquisition considerations. The third area is more technical, system or program oriented at the Command hierarchy. And, finally, the last area speaks of sustainment. Major future initiatives in these areas are reflected in the following paragraphs.

7.1 Organizational Initiatives

Goal: Enable all appropriate decision makers to successfully achieve information dominance.

Modern information resources are expanding at a rapid rate along with accelerated opportunities for IO. All organizations are increasingly reliant upon information, information systems, and must conform to evolving information practices and therefore will be involved in or be susceptible to information warfare. The DoD must be devoted to achieving superior capabilities to survive and win in information warfare. While some organizations within the DoD are responsible for core IO competencies such as technical development, acquisition management, capabilities introduction, technical intelligence, and training and awareness, information warfare has implications and responsibilities across all missions and impacts every

Deleted: 26

DoD organization. Therefore, each DoD activity, organization, and staff should increase their awareness of the opportunities afforded and risks incurred through information warfare. Awareness, education, and training resources will be developed, and provided by DoD core IO organizations to assist in satisfying the goal of building Navy and Marine Corps organizational IO awareness. Awareness is the first step in developing organizational capabilities to employ information warfare successfully in accomplishing missions. All DoD organizations should establish IO coordination positions to obtain IO reference materials, focus IO awareness, training and assistance, and support organization's IO initiatives and activities. Organizations should employ approved information system and network protection tools and practices. They should plan for the use of embedded capabilities for exploitation and offensive information warfare missions when assigned. [Curts, 2000]

7.2 Programmatic / Acquisition Initiatives

Goal: IW opportunities and risks must be considered in the design, acquisition, accreditation, and employment of information based systems for the DoD.

To the maximum extent practicable, the acquisition process for information based systems must take into consideration compatibility issues with other embedded systems, ensure that they are interoperable with Army and Air Force systems / architectures, and incorporate capabilities for protection against IW exploitation and attack. To maximize IW protection, vulnerability assessment must be conducted and considered in program acquisition, beginning during concept development and carrying through installation and accreditation.

7.3 Command Hierarchy Initiatives

Goal: The common tactical picture must be readily available to those who need it which, at one level or another, is virtually everyone.

Today, DoD tends to describe the ultimate goal as "Shared Understanding" or "Shared Awareness." While the authors agree in principle, human nature suggests that the concept of shared understanding may to be a bit out of reach. The best that we can hope for is shared information which will hopefully result in a shared awareness of the situation. There needs to be some acknowledgement that the understanding or awareness being shared is not necessarily identical from individual to individual. Ideally, everyone within the command hierarchy should somehow come to an understanding that everyone else is not only seeing the same picture but is interpreting and understanding it the same way. Assuming all data are interpreted correctly is an extremely high risk to take. This is certainly an area that will eventually include M2M (Machine-to-Machine) cognitive decision-making and is wide open for further research.

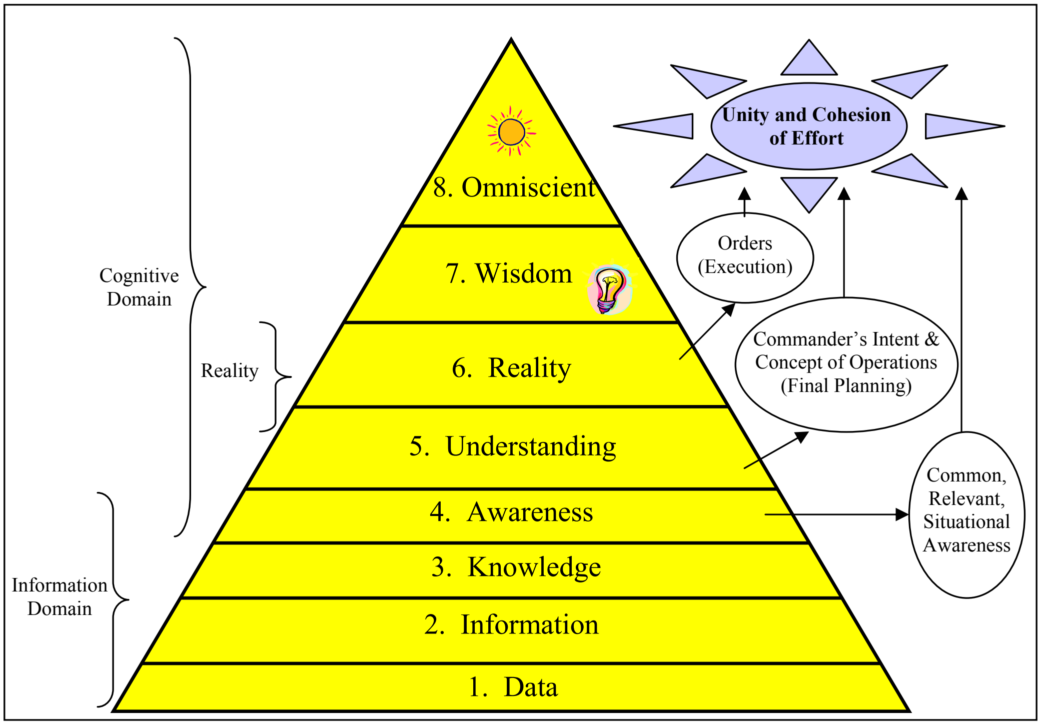

Figure 7: Data Flow Through the Command Hierarchy

7.4 Sustainment Initiatives

Goal: We must find a way to make architecture development and analysis a viable effort over the entire life cycle rather than short-lived initiatives.

A final note on the sustainability of the architectures and the architecture process is in order here. In the authors' view this is the single most important issue in architecture development today and the biggest failing of all such efforts to date. The architecture process (data collection, assessment, option development, design, testing and acquisition) is ***NOT*** a short term effort but rather a very long-term, repetitive process. To the authors' knowledge, no automated architecture assessment process has managed to stay alive through more than one or two iterations and capture the underlying data necessary for a truly repeatable, defendable, robust assessment. Because of the shear magnitude of the effort and the vast amounts of data that must be collected, the first iteration is typically at a very high level and is, most often, rather subjective. Since the time and resources expended to collect and manipulate the data tend to grow rapidly, and because of the short lived nature of the tenure of individual proponents, the process tends to whither away before it has a chance to make the major impact that it is capable of making. If we take the time to investigate the significant impact that some small, short-lived initiatives have had in the past, it would be intuitively obvious to the most casual observer that the concepts, processes and methodologies associated with architecture development and

Deleted: 26

analysis have merit and would significantly increase the effectiveness and efficiency of our acquisition process.

At this writing several such architecture processes are in place and are actively involved in the assessment of DoD programs. What remains to be seen is whether or not the tools, processes and procedures can withstand the test of time.

Deleted: 26

REFERENCES

[Alberts, 2003] Alberts, David S. and Richard E. Hayes. Power to the Edge. Washington, DC: U.S. Department of Defense, Command & Control Research Program (CCRP), 2003.

[Andrews, 1990] Andrews, Timothy, and Craig Harris. “Combining Language and Database Advances in an Object-Oriented Development Environment.” Readings in Object-Oriented Database Systems, 186-196. Stanley B. Zdonik and David Maier, eds. San Mateo, CA: Morgan Kaufman, 1990.

[CIA, 1993] Central Intelligence Agency (CIA). A Consumer’s Guide to Intelligence. Washington, DC: CIA, 1993.

[CMC, 1995] CMC/CNO Memorandum. Information Warfare / Command and Control Warfare (IW/C2W). 16 February 1995.

[Coad, 1990] Coad, Peter, and Edward Yourdon. Object-Oriented Analysis. Englewood Cliffs, NJ: Yourdon Press, 1990.

[Coleman, 1994] Coleman, Derek, et. al. Object-Oriented Development: The Fusion Method. Englewood Cliffs, NJ: Prentice Hall, 1994.

[Cox, 1986] Cox, Brad J. Object Oriented Programming. Reading, MA: Addison-Wesley, 1986.

[Cox, 1987] Cox, Brad J. “Message/Object Programming: An Evolutionary Change in Programming Technology.” Tutorial: Object-Oriented Computing, Volume I: Concepts, 150-161. Gerald E. Peterson, ed. Washington, DC: Computer Society Press, 1987.

[Curts, 1989a] Curts, Raymond J. A Systems Engineering Approach to Battle Force Architecture. Fairfax Station, VA: Strategic Consulting, Inc. (SCI), 1989.

[Curts, 1989b] Curts, Raymond J. An Expert System for the Assessment of Naval Force Architecture. Fairfax Station, VA: Strategic Consulting, Inc. (SCI), 1989.

[Curts, 1999] Curts, Raymond J., and Campbell, Douglas E. “Architecture: The Road to Interoperability.” Paper presented at the 1999 Command & Control Research & Technology Symposium (CCRTS), U.S. Naval War College, Newport, RI, June 29 - July 1, 1999.

[Curts, 2000] Curts, Raymond J., and Campbell, Douglas E. “Naval Information Assurance Center (NIAC): An Approach Based on the Naval Aviation Safety Program Model.” Paper presented at the 2000 Command & Control Research &

Deleted: 26

Technology Symposium (CCRTS), U.S. Naval Postgraduate School, Monterey, CA, June 24 - 28, 2000.

[Curts, 2001] Curts, Raymond J. and Douglas E. Campbell. Avoiding Information Overload Through the Understanding of OODA Loops, A Cognitive Hierarchy and Object-Oriented Analysis and Design. Annapolis, MD: C4ISR Cooperative Research Program (CCRP), 2001.

[DISA, 2004] From the Defense Information Systems Agency website located at: http://www.disa.mil/ns/gig.html

[Dittrich, 1986] Dittrich, Klaus R. "Object-Oriented Database Systems: The Notion and the Issue." International Workshop on Object-Oriented Database Systems. Washington, DC: Computer Society Press, 1986.

[DODD, 2003] Department of Defense Directive 5000.1, The Defense Acquisition System, Office of the Under Secretary of Defense for Acquisition and Technology (USD(A&T)), May 12, 2003.

[DODI, 2003] Department of Defense Instruction 5000.2, Operation of the Defense Acquisition System, Office of the Under Secretary of Defense for Acquisition and Technology (USD(A&T)), May 12, 2003.

[DSBGS, 1993] Report of the Defense Science Board Task Force on Global Surveillance. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology (USD(A&T)), December 1993.

[DSBIAB, 1994] Report of the Defense Science Board Task Force on Information Architecture for the Battlefield. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology (USD(A&T)), 1994.

[DSBR, 1994] Report of the Defense Science Board Task Force on Readiness. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology (USD(A&T)), June 1994.

[Fowler, 1997] Fowler, Martin with Kendall Scott. UML Distilled: Applying the Standard Object Modeling Language. Reading, MA: Addison-Wesley, 1997.

[Hutcherson, 1994] Hutcherson, Norman B., LtCol USAF. "The Five Pillars of Command and Control Warfare," and "Command and Control Warfare—As A War-Fighter's Tool." *Command and Control: Putting Another Tool in the War-Fighter's Data Base*, a research report for Air University Press, Maxwell Air Force Base, Alabama, 1994.

[IWIP, 1996] Curts, Raymond J. and Charles Ristorcelli. Information Warfare Program Directorate (PD-16). Information Warfare Implementation Plan and

Deleted: 26

Acquisition Strategy. Washington, DC: Space & Naval Warfare Systems Command (SPAWAR), 1996.

[IWMP, 1996] Curts, Raymond J. and Charles Ristorcelli. Information Warfare Program Directorate (PD-16). Information Warfare Master Plan. Washington, DC: Space & Naval Warfare Systems Command (SPAWAR), 1996.

[IWS, 1996] Curts, Raymond J. and Charles Ristorcelli. Information Warfare Program Directorate (PD-16). Information Warfare Strategy. Washington, DC: Space & Naval Warfare Systems Command (SPAWAR), 1996.

[JCS, 1996] Joint Chiefs of Staff Brochure, *Information Warfare: A Strategy for Peace, the Decisive Edge in War.* Washington, DC. December, 1996: 19 pp.

[JP 1-02] Joint Chiefs of Staff (JCS) Publication 1-02. The DoD Dictionary of Military and Associated Terms. Washington, DC: U.S. Joint Chiefs of Staff.

[JP 3-13] Joint Publication 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W).*

[Kim, 1989] Kim, Won and Frederick H. Lochovsky, eds. Object-Oriented Concepts, Databases, and Applications. Reading, MA: Addison-Wesley, 1989.

[Kim, 1990] Kim, Kyung-Chang. "Query Processing in Object-Oriented Databases." Lecture Notes. Auston, TX: University of Texas, 1990.

[King, 1986] King, R. "A Database Management System Based on an Object-Oriented Model." Expert Database Systems: Proceedings of the 1st International Workshop. Larry Kerschberg, ed. Menlo Park, CA: Benjamin Cummings, 1986.

[Kuehl, 1997] Kuehl, Dan. "Defining Information Power." *Strategic Forum*, Number 115, National Defense University, Institute for National Strategic Studies, June 1997.

[Libicki, 1995] Libicki, Martin C. "What Is Information Warfare?" *Strategic Forum*, Number 28, National Defense University, Institute for National Strategic Studies, May 1995.

[Manola 1987] Manola, Frank A. "PDM: An Object-Oriented Data Model for PROBE". Cambridge, MA: Computer Corp. of America, 1987.

[Molander, 1996] Molander, Roger C. et. al.. "Strategic Information Warfare: A New Face of War." *Parameters*, Autumn 1996, U.S. Army War College, Carlisle Barracks, PA.

Deleted: 26

[MOP 30] Chairman, Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) #30. Command and Control Warfare (C2W). Washington, DC: U.S. Joint Chiefs of Staff, 8 March 1993.

[NDP 6] Naval Doctrine Publication #6. Naval Command and Control. Washington, DC: U.S. Navy, 1 September 1994.

[NISL Pub 1] Naval Information System Library, Publication #1. The Rise of Modern Command and Control. Washington, DC: The Renaissance Group of Washington, DC, 1995.

[RMC, 1995] Report of the Commission on Roles and Missions of the Armed Forces. Directions for Defense. Arlington, VA: U.S. Department of Defense (DoD), 1995.

[Sage, 1991] Sage, Andrew P. Decision Support Systems Engineering. New York, NY: John Wiley & Sons, Inc., 1991.

[Smith, 2002] Smith, Edward A. Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War. Washington, DC: U.S. Department of Defense, Command & Control Research Program (CCRP), 2002.

[Taylor, 1997] Taylor, David A. Object Technology: A Manager's Guide, 2nd Ed. Reading, MA: Addison-Wesley, 1997.

[Thomas, 1990] Thomas, Agrawal, Jajodia and Kogan. "A Survey of Object-Oriented Database Technology." Fairfax, VA: George Mason University, 1990.

[Zaniolo, 1986] Zaniolo, Ait-Kaci, Beech, Cammarata, Kerschberg and Maier. "Object Oriented Database Systems and Knowledge Systems." Expert Database Systems: Proceedings from the 1st International Workshop. Larry Kerschberg, ed. Menlo Park, CA: Benjamin Cummings, 1986.

Deleted: 26