Information Warfare, INFOSEC, and Dynamic Information Defense*

J.R. Winkler, C.J. O'Shea, M.C. Stokrp

PRC Inc.
1500 PRC Drive
McLean, VA 22102
(703) 556-1000
winkler_vic@prc.com oshea_connie@prc.com stokrp_mark@prc.com

ABSTRACT

This paper surveys issues and requirements for future Information Warfare (IW), and introduces our concepts for an area we call: "dynamic information defense" [1]. Although defensive IW would incorporate relatively static information security (INFOSEC) capabilities, an effective IW defense must survive exploitation of pervasive "weak links" in security. This demands countermeasures of a fundamentally more dynamic, cooperative, and distributed nature than are available today. As described in this paper, dynamic information defense transcends INFOSEC with a broader strategy that integrates planning and analysis with a means for situational intelligence to achieve robust in-depth information defense.

1 INTRODUCTION

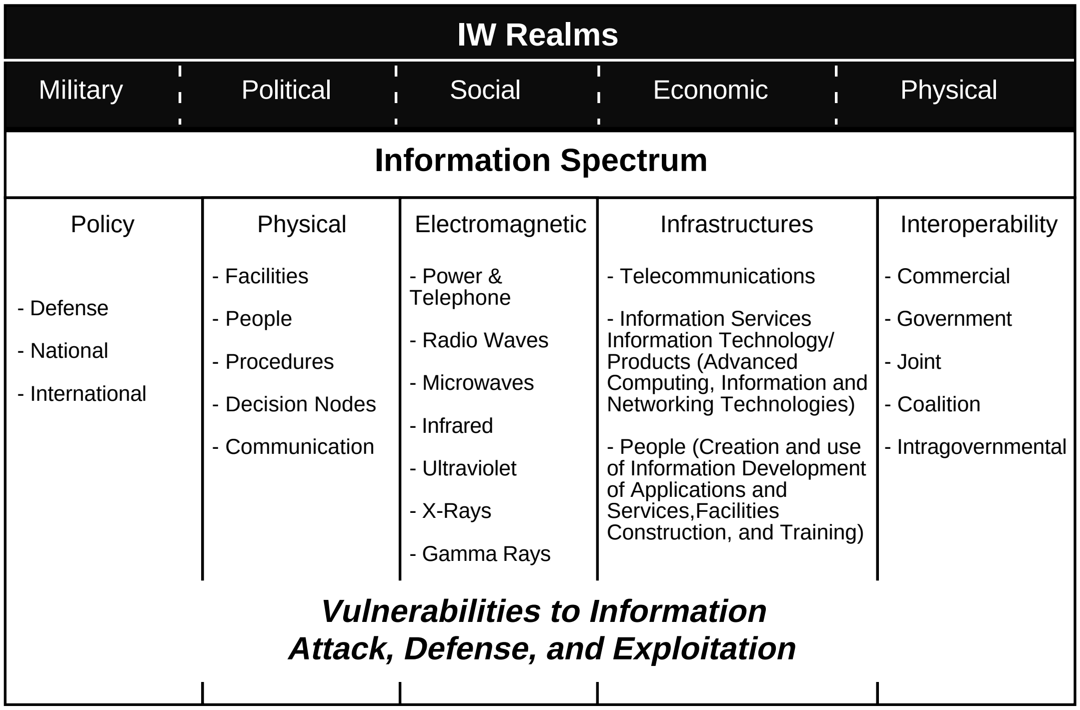
The information age has brought changes that challenge our ability to ensure the availability, integrity, and security of systems and information infrastructures [2]. New technologies and information needs exceed the state-of-the-art, let alone the state-of-the-practice, in information assurance and information security (INFOSEC). The predominant security models and implementations of the 1980s were oriented toward securing single monolithic systems. In the main, INFOSEC did not anticipate the nature of, and did not meet the security needs for computing in the 1980s. For instance, the development of windowing systems challenged trusted operating systems to maintain the classification levels of documents. Likewise, the rapid rise of networks, desktop computers, and workstations resulted in a decentralization of control over information resources that challenged information security practices and capabilities.

In the 1990s, advances in performance, multimedia, internetworking, and hypertext — combined with the phenomenal appeal of the WWW — have resulted in the seemingly universal desire to interconnect networks in order to disseminate or access information. Recent computing trends have brought further challenges as technology continues to evolve. INFOSEC challenges in the 1990s include meeting requirements that may conflict, such as the need for high-assurance protection, while concurrently simplifying access to information. Similarly, having a means to trust information sources and identities can run counter to the need to assure information privacy.

* We define the term *dynamic information defense* as: An integrated set of automated, flexible countermeasures used to facilitate IW threat detection and to dynamically plan, monitor, and control a range of coordinated responses.

As information infrastructures become increasingly interdependent and complex, we also grow increasingly dependent upon them. These systems have shown vulnerabilities to attack and exploitation [3, 4]. If our information defenses do not evolve to meet continued technological advances, then we will not be able to meet emerging information needs with information infrastructures that can withstand offensive or exploitative threats.

Information Warfare (IW) [5] is motivated by the opportunities that arise from an ever increasing dependence upon vulnerable information systems. IW is the information age battlefront whose scope circumvents physical and electronic defenses which extend throughout the IW realms of Military, Political, Economic, Social, and Physical. Each realm consists of a complex, interdependent infrastructure of systems and processes that are subject to attack and exploitation by a range of adversaries. As shown in Figure 1, each IW realm is based upon the information spectrum—Policy, Physical, Electromagnetic, Infrastructures, and Interoperability. Specific vulnerabilities to a realm occur throughout the information spectrum; therefore, vulnerabilities unique to each piece of the spectrum are subject to attack or exploitation. Regardless of borders or geography, all digital information assets are at least potentially vulnerable to IW threats [6].



IW Realms

Military	Political	Social	Economic	Physical

Information Spectrum

Policy	Physical	Electromagnetic	Infrastructures	Interoperability
- Defense - National - International	- Facilities - People - Procedures - Decision Nodes - Communication	- Power & Telephone - Radio Waves - Microwaves - Infrared - Ultraviolet - X-Rays - Gamma Rays	- Telecommunications - Information Services Information Technology/ Products (Advanced Computing, Information and Networking Technologies) - People (Creation and use of Information Development of Applications and Services,Facilities Construction, and Training)	- Commercial - Government - Joint - Coalition - Intragovernmental

Vulnerabilities to Information Attack, Defense, and Exploitation

Figure 1 — The Information Spectrum and IW Realms

To achieve a specific objective, a given information system may be targeted directly or indirectly. Likewise, in pursuit of tactical goals, an IW attack could exploit the dependency of a targeted system on one or more of its enabling components [7]. IW threat vectors will evolve as processing power, storage capacities, and network bandwidth and connectivity continue to advance.

While a low-technology IW attack only needs to exploit a subset of the vulnerabilities, a medium, or high technology IW attack would likely overwhelm targeted systems and infrastructures. Today, we have only rudimentary, semi-automated, and human-intensive means for countering these threats. While technology which poses IW threats need only be simple and unsophisticated, effective countermeasures are easily orders of magnitude more difficult to implement.

Consequently, there is a clear need for flexible and responsive IW capabilities that form an integrated set of automated countermeasures. These must transcend information defense and should implement the information-age equivalent of the appropriate ‘counter’ disciplines. Not only will such countermeasures need to facilitate detection, but they must also be able to dynamically affect a range of coordinated defenses. Such countermeasures are themselves prone to exploitation and attack, leading to a cycle that may be similar to counter-counter-escalation in the realm of Electronic Warfare (EW).

The remainder of this paper presents a high-level overview of our concepts and approach for an area we call: "dynamic information defense." Section 2 surveys the basic principles of INFOSEC and presents a brief background on IW. Section 3 identifies the essential issues for a future information war in terms of requirements and technologies. We discuss our concept of "dynamic information defense" and outline the requirements of a strategy for in-depth information defense. These are shown to be significantly broader in scope than static INFOSEC countermeasures. Section 4 outlines our principal research goals.

2 BACKGROUND

While INFOSEC is oriented toward information assurance or protection, IW is by definition more dynamic and demands robust and flexible means for information attack, exploitation, and defense. Today, information defense failures, insufficient mechanisms, and insufficient defense strategies are common in INFOSEC. These defenses are typically static in nature, feature minimal flexibility, offer limited reaction capabilities, and they are typically standalone and not coordinated beyond a narrow range of functionality.

In contrast, on the battlefield, when positional defense fails, a commander has a range of options to include counterattack in order to retake seized ground, or a defense in-depth to not only retake terrain, but to also inflict maximum damage to the enemy by channeling initial attacks into killing zones. Similarly, intelligence officers respond when security is breached by a hostile intelligence services agent, typically by attempting to double the source, thereby turning an otherwise intelligence disaster into an advantage.

To meet the challenges of comparable IW situations requires significant advances in information defense countermeasures. As explained next, although existing INFOSEC countermeasures have a comparatively primitive and narrow range of reaction capabilities, they are necessary within a much broader and augmented defensive IW framework.

2.1 INFOSEC

Briefly, INFOSEC is concerned with protecting information against failure, error, attack, and catastrophe with the goal of preventing denial of service, improper disclosure, modification, or destruction of information. INFOSEC countermeasures are generally oriented toward defending systems from known or somewhat predictable threats. The process of selecting countermeasures is usually driven either by high-level policy or by a cost-benefit tradeoff to assess vulnerabilities and analyze risks.

However, in terms of the threats posed by IW against countermeasures, neither the state-of-the-practice nor the state-of-the-art in INFOSEC are prepared to address the challenges of defense against IW attack. This is because INFOSEC countermeasures, such as trusted operating systems, guards, firewalls, network monitoring, and intrusion detection tend to be:

- Orientated toward known threats or vulnerabilities and tend to address single vulnerabilities, versus being active defenses against new or multiple vulnerabilities that may be exploited in concert;
- Difficult to configure for accurate and reliable operation and typically are not updated in response to changes to the computing environment or threat vectors;
- Functionally limited and inflexible, and rarely include significant information or knowledge about the protected domain. While such capabilities as domain name services, audit-based intrusion detection systems, and network routers maintain more information about their environments, even these are limited in responding to security situations by changing their missions or rule-bases; and
- Lacking all but rudimentary interoperability or information sharing capabilities and rarely leverage situational information from a given domain or exchange threat information with other systems.

These and other limitations, make it impossible to construct an effective IW defense solely on such countermeasures. In an IW campaign, we should expect a maelstrom of threats whose particular form can not be fully anticipated in advance and which would likely change as we reacted to them.

2.2 IW

Development of an effective IW defense can be considered analogous to the development of Command, Control, and Communications Countermeasures (C^3CM) [8]. In the 1970s the Soviets advanced their concept of Radio-Electronic Combat (REC) [9]; the US response was the development of C^3CM. C^3CM is often advanced as a forerunner of Command and Control Warfare (C^2W) [10,11] — the DoD implementation of IW. It is important to clarify the relative demands of C^3CM (an industrial age, single threat, technology driven concept) vis-à-vis the greater demands of C^2W (a post-cold war, information age vision). First, C^3CM was primarily based on a philosophy that "the best defense is an attack." It was limited in its attack-protect balance. Second, it was oriented on communications as not only a main means of implementation, but as the best one. C^3CM lacked a synergistic and simultaneous approach to information as the key. Lastly, C^3CM addressed the tactical-operational environment during hostilities—but only within the theatre of operations. Little or no consideration was given to pre-hostilities conditioning, post-hostilities requirements, or relevant information intelligence within a global context.

In contrast, C^2W is built upon five pillars and is supplemented by intelligence support, as shown in Figure 2. We recognize the importance of Relevant Information Intelligence (RII) [12], and identify three additional classes of intelligence information as necessary for IW, C^2W, and a dynamic information defense. These classes are:

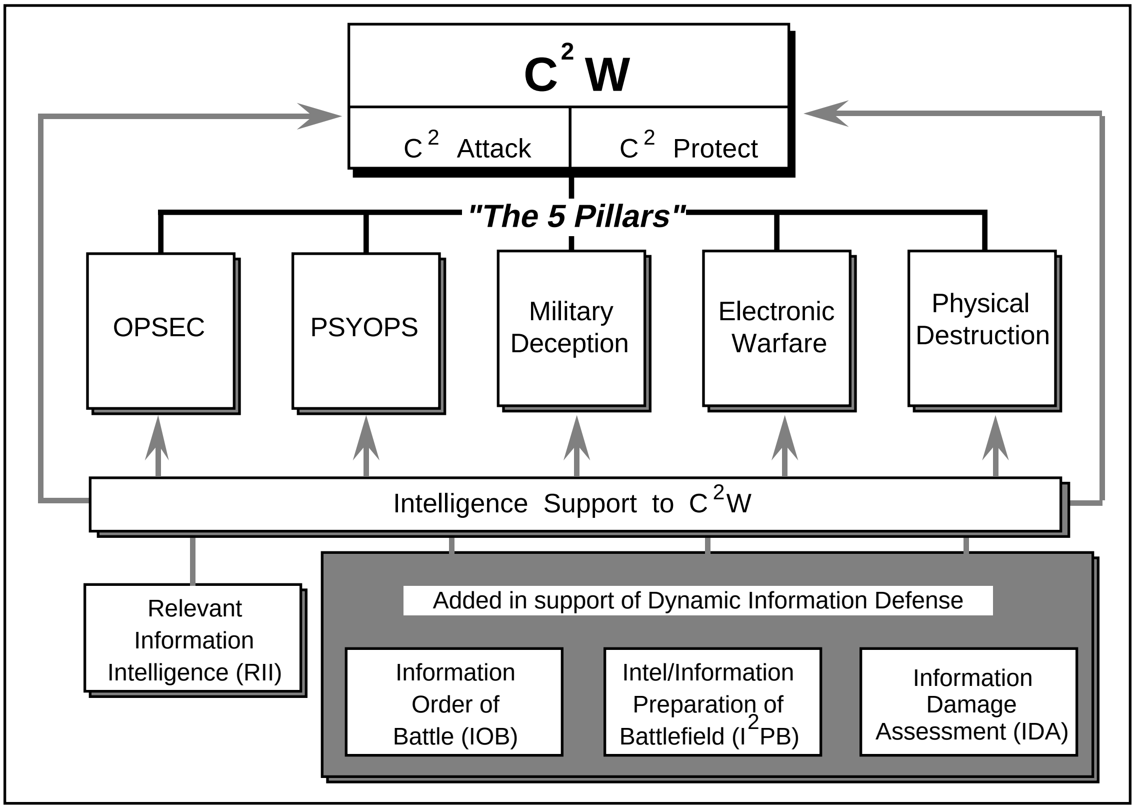

C 2 W
C 2 Attack
C 2 Protect
"The 5 Pillars"
OPSEC
PSYOPS
Military Deception
Electronic Warfare
Physical Destruction
Intelligence Support to C 2 W
Relevant Information Intelligence (RII)
Added in support of Dynamic Information Defense
Information Order of Battle (IOB)
Intel/Information Preparation of Battlefield (I 2 PB)
Information Damage Assessment (IDA)

Figure 2 — The Pillars of C^2W

- Information Order of Battle (IOB) — we define IOB as: the command, mission, and information flow structure of any military force as well as all enabling information infrastructures. C^2W, operational security (OPSEC), and targeting in IW often extend beyond the commanders area of influence and thus require a greater degree of coordination at higher levels;
- Intelligence/Information Preparation of Battlefield (I^2PB) — we define I^2PB as: the incorporation of RII and IOB into IPB to enhance the waging of information-based warfare; and

- Information Damage Assessment (IDA) — we define IDA as: the automated identification, assessment, and reporting of information attack or information exploit attempts.

Significant differences exist between C^3CM and C^2W. Just in terms of C^2W objectives, consider the magnitude and relevance of these to the evolution of C^2-attack and C^2-protect. These are to cause or force:

- An adversary to make a substantive decision favorable to exploitation by oneself (e.g., changes in force allocation or plans via disruption or destruction);
- An adversary to make changes in their planned time lines favorable to exploitation by oneself (e.g., delays via disruption, destruction, or manipulation);
- An adversary to make a decision favorable to oneself (e.g., degradation of offensive capabilities in a particular locale via deception or perception management);
- Gridlock in an adversary's decision making capabilities, while our own remain intact (e.g., simultaneity in destruction, disruption, and deception); and
- An adversary into accepting situations or conditions that are contrary to their objectives (e.g., terrorist's imposition of their demands or a nation state's deterrence through information power or some combination of national power employing information).

The information process and the decision/C^2 process [13] are fundamental to achieving the objectives of C^2W. This is done by utilizing the total information spectrum throughout the IW realms, and across the time line that encompasses pre-hostilities, hostilities, and post-hostilities. Just as the information spectrum is not solely dependent upon the electromagnetic spectrum, neither is the military IW spectrum solely dependent upon military assets. In IW, when several threat vectors are used, perhaps in conjunction with Dominant Battlespace Awareness (DBA) targeting, the result can be the overwhelming application of precision force.

From the discussion above, it is evident that the practice of INFOSEC and existing countermeasures are not sufficient to meet the needs of IW or the objectives of C^2W. Survival in an IW theatre demands countermeasures much broader in functionality and more advanced than existing ones.

3 Future IW: Issues and Requirements

Today, a commander's actions can no longer be governed only by what he controls in a theater of operations. He operates in a global infosphere where vulnerabilities to IW attack are spread across all realms. To ensure military success or dominance in IW, we must address this fact. Where information systems are critical—and vulnerable to attack—countermeasures equal to the task need to be in place.

The tempo and scope of an IW attack entails near-real-time (NRT) defense capabilities. Countermeasures need to respond to existing threats, combinations of threats, and emerging threats. Thus, we require countermeasure functionality that can not always be fully defined in advance of attack. In our estimation, IW defense will require countermeasures that are automated, dynamic, flexible, adaptive, and that not only survive but dominate threats. In part, this will require significant advances in computing technology, particularly in such areas as intelligent agents, adaptive systems, and the systems equivalent of OPSEC.

Defensive IW needs to detect, analyze, plan, and control counter attacks. It must be effective despite uncertainties, chaos, and failures that are common in operational situations. A timely, coordinated, and robust response to threats requires a range of command and control functionality that spans centralized, cooperative, and independent operation—throughout the information spectrum and across each IW realm.

3.1 Dynamic Information Defense

The implementation of information assurance throughout the information spectrum requires full counterpart objectives, organization, doctrine, and technology. This can be classified as an in-depth information defense strategy. In contrast to a typical information defense that is vulnerable to, and unlikely to survive compromise of a single weak link, an in-depth information defense strategy includes additional defenses.

We define the term *dynamic information defense* as: an integrated set of automated, flexible countermeasures used to facilitate IW threat detection and to dynamically plan, monitor, and control a range of coordinated responses. Implementing this entails a combination of centralized and distributed IW capabilities to execute the overall information defense mission. Individually, distributed countermeasures would be tasked to mitigate a variety of threats. Thus, we see a need for flexible and intelligent countermeasures, which can satisfy the need for defenses to augment and extend existing INFOSEC countermeasure capabilities.

Our dynamic information defense paradigm revolves around planning and analysis capabilities. This is driven by the needs of activities such as advance planning, IDA, and countermeasure cooperation. These require planning and analysis and a means to disseminate information associated with these activities. In contrast to the static nature of a traditional INFOSEC vulnerability assessment, IW and dynamic defense activities demand a continuous cycle of information and OPSEC database updating. Information of various classes (such as discussed in Section 2) is required, this includes: RII, IOB, IDA, and I^2PB.

Figure 3 is an overview of our paradigm for dynamic information defense and depicts the perimeters of an information defense in-depth. First, an OPSEC analysis is required to determine known or anticipated vulnerabilities within the information spectrum, the IW realms, and the conflict time-line.

Next, vulnerabilities are addressed with INFOSEC countermeasures. Within a dynamic defense, these countermeasures must become more sophisticated, and should include embedded support for:

- Interoperable encryption as a basic foundation for trusted communications;
- Unforgeable and untamperable identification, for mutual trust, non-repudiation, and OPSEC;
- Untamperable trusted components, including: secure kernels, intrusion detection rule-bases, and security monitoring systems; and

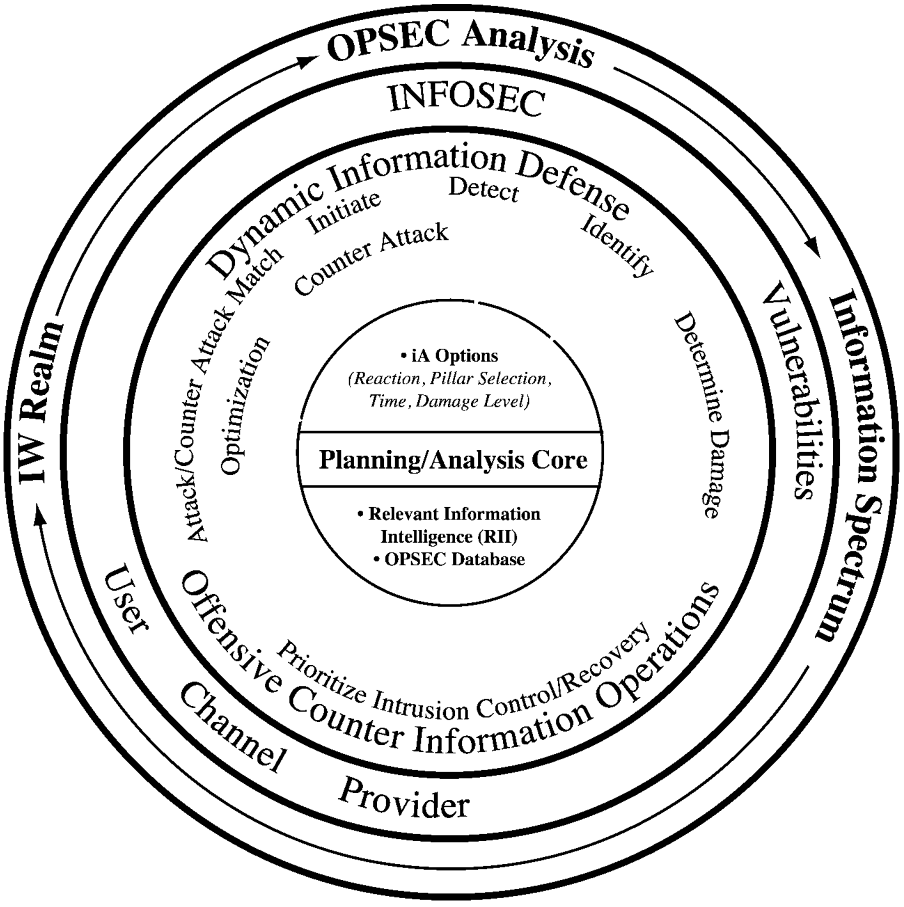

OPSEC Analysis
INFOSEC
Information Spectrum
Vulnerabilities
IW Realm
User
Channel
Provider
Dynamic Information Defense
Initiate
Detect
Identify
Counter Attack
Attack/Counter Attack Match
Optimization
Determine Damage
Offensive Counter Information Operations
Prioritize Intrusion Control/Recovery
• iA Options
(Reaction, Pillar Selection, Time, Damage Level)
Planning/Analysis Core
• Relevant Information Intelligence (RII)
• OPSEC Database

Figure 3 — Information Defense In-Depth Paradigm

- Capabilities for wide-area monitoring of networks, along with a basic means or strategy for the automated generation and communication of situational intelligence.

Dynamic information countermeasures are central to achieving a second and significantly more capable line of defense. While having a partial foundation in INFOSEC, dynamic information defense entails the adaptation of traditional counter disciplines and the use of intelligent components, such as intelligent agents (iAs). In this context, dynamic information defense capabilities would:

- Augment existing countermeasures with dynamic and reconfigurable elements for countering threats that are outside the scope of, that would compromise, or circumvent INFOSEC;
- Implement NRT information damage assessment (IDA) or compromise [14];
- Implement a secure means of inter-communication between countermeasures for dissemination of defense plans, situational information, and cooperation;
- Be implemented with both centralized and distributed components—the distributed components would likely include iA or related technology and would be capable of being dynamically tasked according to an OPSEC database or a disseminated information defense plan [15]; and
- Use an OPSEC database to support both the centralized and distributed defense components.

Consistent with C^2W, it may prove necessary to include offensive counter information operations (OFCIOs)—the military equivalent of counterattacking [16] within a defense in-depth area of operations. Within this context, the objectives for OFCIOs would be to:

- Ascertain offensive information operations modus operandi (MO) of adversaries to enhance planning and direction for future information counterattacks;
- Use and redirect an attack to tie-up an adversaries information resources;
- Redirect information attacks to influence and assist friendly operations.

To implement OFCIOs within our dynamic information defense paradigm, we would consider the following factors:

- A reaction course of action (i.e., selection of whether to negate the attack or exploit it through dynamic information defense and specifically OFCIOs);
- A C^2W pillar course of action (i.e., selection of which C^2W pillar will be used for counterattack, for example, disruption of an adversary information system by reversal or deception);
- A time course of action (i.e., whether a counterattack should be immediate or delayed); and
- A damage level course of action (i.e., should a counterattack be gradual or catastrophic).

Clearly, IW is significantly broader in scope than INFOSEC. To a great extent, the range of IW activities are defined by the five C^2W pillars. Our concept of a dynamic information defense is consistent with both IW and the C^2W pillars. This model for a dynamic information defense is a response to the needs of IW defense and the shortcomings of INFOSEC to meet those needs.

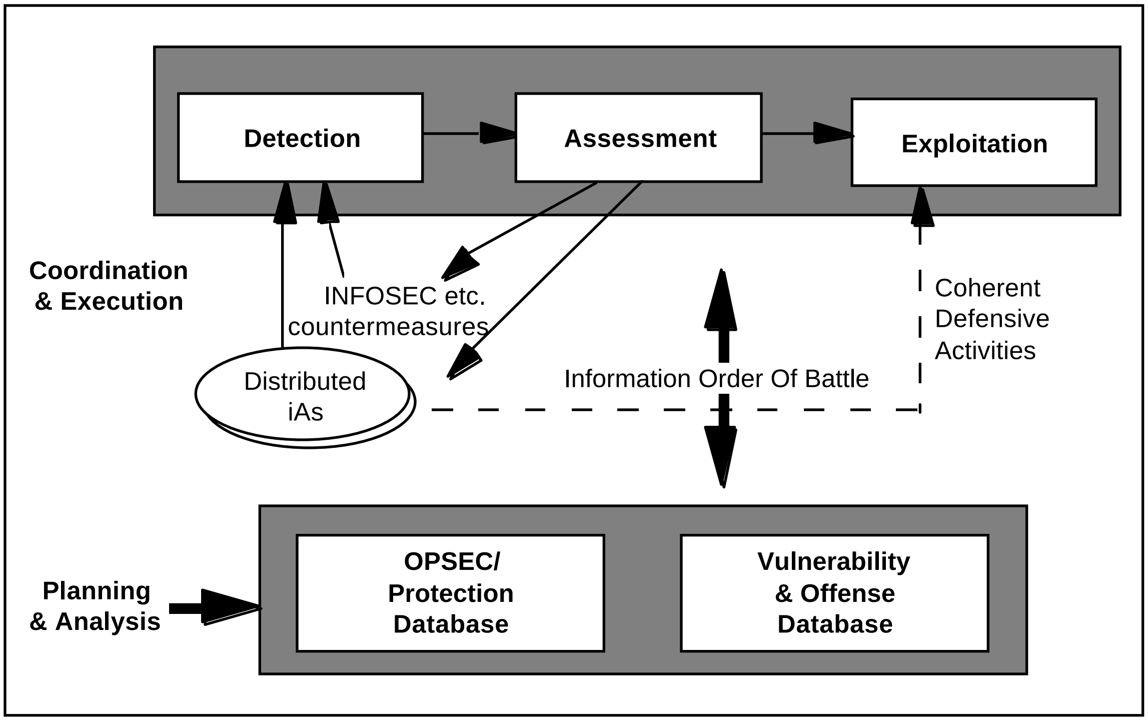
4 RESEARCH CONCEPT

Our research focus is on defensive and exploitative IW. The objective is to develop tools to facilitate C^2W efforts under a broader IW campaign. Such capabilities are necessary to counteract an adversary from exploiting, corrupting, and otherwise benefiting from access to our infosphere.

At this time, we have defined the overall project goals and objectives, and developed the functional architecture shown in Figure 4. This architecture is consistent with our information defense in-depth paradigm discussed earlier. We have also begun proof-of-concept prototyping. The principal underlying software technologies include intelligent software agents and Java.

Our prototype is designed to address vulnerabilities in the computing infrastructure and in compromise of critical information that could be exploited. It supports centralized C^2, and features intelligent, automated tools to facilitate planning and analysis for decentralized execution. The prototype is being developed in a distributed, networked environment and features dynamic and flexible IW countermeasures. These are designed to be rapidly reconfigurable to meet and respond to changes in threats. Individual countermeasures may cooperate in pursuit of an overall IW defense as well as in tactical and strategic objectives. For instance, iAs may be deployed among critical nodes, or functional components, that may be associated with or are IW targets. By considering criteria such as risks and vulnerabilities, a component's value as a target to the enemy, and a component's value as an asset to our own warfighters, the decision of when and where to deploy iAs can be made.

Intelligent agents will be used to perform a variety of tasks to defend against IW threats. They will support traditional INFOSEC functions by performing tasks such as monitoring firewalls and guards, and analyzing network traffic. Such monitoring information then can be leveraged for broader indications and warnings (I&W) and for the dissemination of knowledge about observed IW attack capabilities. This is seen as critical to a coordinated and robust defense. Further, iAs can provide the enhanced capabilities needed by detecting, observing, analyzing, and reporting on previously undefined offensive IW attacks. In response to detected attacks, the iAs may respond:



Detection
Assessment
Exploitation
Coordination & Execution
INFOSEC etc. countermeasures
Distributed iAs
Information Order Of Battle
Coherent Defensive Activities
Planning & Analysis
OPSEC/ Protection Database
Vulnerability & Offense Database

Figure 4 — Functional Architecture for Dynamic Information Defense

- Independently in accordance with previously defined scenarios (stored in an OPSEC database);
- In concert with other deployed iAs; and
- In concert with the Central Coordinating Facility (CCF), discussed next.

The final component of the prototype is the CCF, which directly supports IW battle management by:

- Monitoring and displaying IW status;
- Facilitating information damage assessment;
- Providing a dynamic planning and analysis capability to respond to threat situations which could not be fully anticipated or defined in advance of attack;
- Managing the iA knowledge base, which encompasses both the OPSEC database component of previously defined threat response scenarios as well as the database component used to support the dynamic planning and analysis capability;
- Coordinating the execution of responses to detected attacks in concert with deployed iAs;

and

- Facilitating centralized reporting of status and lessons learned.

Within this framework, we intend to prototype various concepts and assess their usefulness in counteracting an adversary’s attempt to exploit, corrupt, and leverage access to our infosphere. If successful, results of our prototyping activities will make a significant contribution toward empowering the warfighter with the means to effectively manage an IW campaign.

5 SUMMARY

It is essential that our information defenses evolve to meet the continued revolution in technological advances and to provide the US with information infrastructures that are able to withstand offensive or exploitative IW threats. Today, neither the state-of-the-practice nor the state-of-the-art in INFOSEC are prepared to address the challenges of defense against IW attack.

This paper has presented a high-level overview of our concepts and approach for the implementation of a dynamic information defense. Since survival in the IW theatre demands countermeasures that are broader in functionality and more advanced than existing INFOSEC capabilities, our concept integrates planning and analysis into an in-depth information defense. To this end, we have begun development of a prototype for an intelligent, distributed, coordinated, and dynamic information defense capability.

Acknowledgments

The authors owe credit to the ideas and efforts of our colleagues: Justin Landry, Julie Lehnertz, and John Page. In addition, thanks are due to Dr. Jude Franklin and Dr. John White for their continued support.

[1] Winkler, J.R. O’Shea, C.J., Stokrp, M.C. "Information Warfare & Dynamic Information Defense", June 1996 Command and Control Symposium, Naval Postgraduate School, Monterey CA. June 1996.

[2] Alberts, Dr. David S., “The Unintended Consequences of Information Age Technologies”, National Defense University, NDU Press Book, April 1996.

[3] Swett, Charles, “Strategic Assessment: The Internet”, Office of The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (Policy Planning), 17 July, 1995

[4] Staff of the Security Policy Board “White Paper on Information Infrastructure Assurance”, December 1995.

[5] IW is defined by the DoD as: “Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks” [Draft DODDIR 3600.1, 1996].

[6] Libicki, Martin C., “The Next Enemy” National Defense University, Strategic Forum, Number 35, July 1995

[7] For instance, the strategic value of an IW attack against one or more of the infrastructures that enable a base-level communications network (such as the power grid, the National Information Infrastructure (NII), the Defense Information Infrastructure (DII), or other non-military communications) could indirectly achieve the equivalent tactical goals as attacking specific computing or communications nodes within the network.

[8] Littlebury, F. E.; Praeger, D. K. “INVISIBLE COMBAT: C^3CM - A GUIDE FOR THE TACTICAL COMMANDER.” Washington DC: AFCEA International Press; 1986; ISBN: 0-916159-11-6.

[9] Hemsley, John. “Soviet Troop Control: The Role of Command and Technology in the Soviet Military System”. Oxford, U.K. and N.Y.: Brasseys Limited, 1982.

[10] Chairman of the Joint Chiefs of Staff. “COMMAND AND CONTROL WARFARE.” ; 1993 Mar 8; Memorandum of Policy No. 30.

[11] Chairman of the Joint Chiefs of Staff. “JOINT DOCTRINE FOR COMMAND AND CONTROL WARFARE (C^2W)” (Preliminary Coordination Draft). ; 1995 May; JOINT PUB

3-13.

[12] Relevant Information Intelligence (RII) — Current intelligence concerning a potential adversaries information capabilities, systems, dependencies, and the status of information infrastructures within an area of operations.

[13] The information process transforms data to information to knowledge. The decision/C^2 process consists of the cycle: observe, orient, decide, act— the OODA loop.

[14] The cycle for accomplishing IDA is: detect, identify, determine damage, and prioritize intrusion control and recovery actions.

[15] We envision several classes of distributed defensive components that are capable of a range of cooperation and information-sharing in support of information defense. These would serve as the automated equivalent of a command hierarchy; i.e., centralized control and decentralized execution.

[16] The cycle for counterattack implementation is: construction of counterattack options (accomplished prior to attack and continually refined), attack/counterattack match optimization, decision and initiation of counterattack.