Vision and Strategy
For Defending Information

by

Lt Col John D. Wright, USAF
Vice Commander, Combined Intelligence Center

The Vision

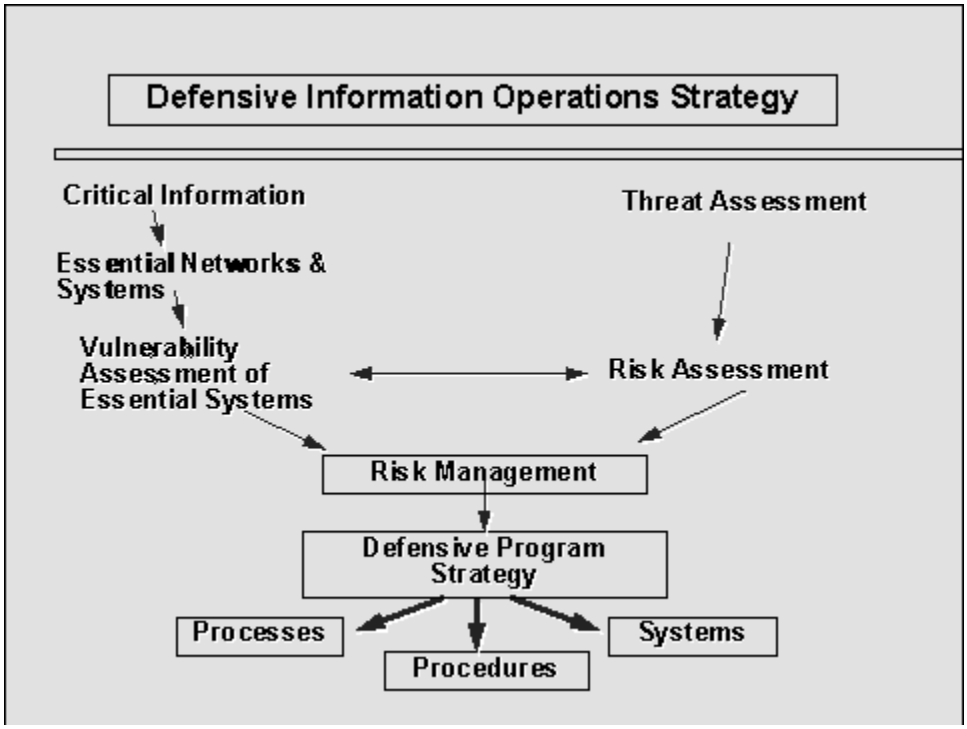
By the first years of the new millenium, a fundamental change in force structure and doctrine has taken place within the US military. A smaller, more technologically proficient force has emerged readily internetted by sophisticated command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR).[1] Information superiority is a primary warfare objective and enhances precision application of force across a very wide range of operations from military conflict to peace keeping. Strategic forces continue to serve as one of the elements of our nation's insurance policy, but they are supplemented as a National and theater deterrent force by both Information Operations and Precision Guided Munitions capabilities. The Defense Information Infrastructure is an integrated whole, dependent and in many ways indistinguishable from the National and Global Information Infrastructures. They support multilateral and coalition operations, and are protected by dynamic, risk-based processes. Defense core expertise supports a national indications and warning center, which provides early notification and mitigation for attempts to manipulate national information processes.

Continued proliferation of low-cost technology, however, has created challenges to U.S. interests from nations with regional ambitions, non-state actors, and criminal elements seeking exploitation opportunities. The threat results in continual attempts to probe, manipulate, degrade and/or destroy our information processes and, as a result, make protection of our information and enabling infrastructure a basic consideration in all phases of acquisition and execution.

Information operations[2] is a formalized warfare discipline at the service and joint command levels, and supports national policy; its concepts have caused changes in doctrine, strategy and organization, resulting in a more streamlined, cost-effective, information-secure force. Previously disparate disciplines like PSYOPs, Deception, Electronic Warfare, precision strike, INFOSEC, COMSEC and OPSEC are integrated to mutually support one another, and produce a single, coherent effect whether in defensive or offensive operations. Common terminology and principles are accepted conventions; service and national war colleges educate senior leadership in its principles. Information Operations strategies are developed across a virtual network of modeling and simulation centers, and are exercised by component and joint forces, continually exploring innovative strategies and concepts. Information Operations tools provides the National Command Authority with a wide range of non-lethal or augmentation options to tactical, theater, or strategic operations, and significantly enhances the effectiveness of limited use of force. Information superiority as well as the supporting integrated information infrastructures are viewed strategically.

The Defensive Information Operations Strategy[3]

The defensive information operations process establishes a baseline of critical data (see diagram); identifies essential networks and systems; and assesses their vulnerability. As this activity proceeds, the threat is assessed and concomitant risk determined based on the vulnerability assessment. This leads to a risk management process, which incorporates cost/benefit analysis to yield a Defensive Program Strategy. Processes, procedures, and system solutions based on technology, design, testing, exercises, and operational employment to support the strategy can then be implemented. The process is dynamic and continues to integrate and refine the strategy and solutions.



This Defensive Information Operations Strategy is a process to manage risk. It is impossible to pay the financial and operational price of total risk avoidance. Risk management provides appropriate protection based on priorities as well as effectiveness and efficiency considerations. The risk management process and resulting strategy must address the interests, capabilities and information systems serving the government, including those provided by the civil sector communities, as well as the role of non-government elements in these complex activities. The strategy will yield a consistent approach and economies of scale in protecting the highly interconnected Defense Information and National Information Infrastructures (DII and NII). These rapidly evolving and highly complex systems require proactive measures to ensure integration and maximum efficiency. The following seven principles will guide this Defensive Information Operations Strategy: 1) Information, information systems, information-dependent systems, infrastructure components, and advanced weapons systems shall be identifiied and evaluated through a risk management process. 2) Command and control of forces shall be planned and exercised to minimize the amount of critical information required for direction and application of force, while taking full advantage of the relevant information that is available to

enhance such direction and application. U.S. forces shall prepare to operate successfully in degraded information and communications environments. 3) Information operations considerations shall be included in all information and weapon systems development and acquisition programs, and integrated into force planning and execution decisions. 4) Continuous interaction and integration among command, control, communications, computers, intelligence, surveillance, and reconnaissance activities shall be incorporated in the requirements, research and development, acquisition and operational processes. 5) The pace of information technology advance far outstrips the current acquisition process' ability to respond and leverage that technology into military systems. The extensive use of commercial-off-the-self (COTS) products by the military provides cost savings opportunities, but entails increased risk management requirements. The acquisition process shall be streamlined consistent with this reduced development timeline while addressing inherent risks and to retain U.S. military readiness and operational capabilities. 6) Computer simulation technologies together with networked wargaming and exercises shall be used to create realistic environments for training, exercise planning, and acquisition purposes. Wargames and exercises should simulate wartime stresses to ensure commanders of U.S. forces both understand and are prepared to operate/exploit information and information system capabilities and vulnerabilities. 7) Service and Agency core competencies shall be sustained and enhanced, while at the same time policy, personnel, technologies, systems architectures, programs, plans, and budget aspects shall be integrated.

Notes

1. Intelligence, Surveillance, and Reconnaissance (ISR) is the capability to collect, process, exploit and disseminate accurate and timely information that provides the battlespace awareness necessary to successfully plan and conduct operations. (AFDD 2-5.2)

2. Information operations: actions taken to affect adversary information and information systems while defending one's own information and information systems. (DoDD S-3600.1)

3. Strategy adapted by work while author was assigned to Assist Sec Def (C3I) Staff, 1994-1996 with J. Spencer and D. Hotard