Information Operations in Support of Civil-Military Interactions [1]

Alexander E.R. Woodcock, Ph.D. [2]

Chief Scientist and Vice President
Synectics Corporation, Fairfax, Virginia, U.S.A.
e-mail: woodcock@syncorp.com

James E. Heath, Ph.D.

Senior Intelligence and Technical Advisor
Land Information Warfare Activity (LIWA)
United States Army Intelligence and Security Command
Fort Belvoir, Virginia, U.S.A.
e-mail: jim@heathmail.com

Alexander (Ted) Woodcock is Chief Scientist and Vice President at Synectics Corporation, Fairfax Virginia. He was recently elected a Member of the Royal Swedish Academy of War Sciences. He is also Guest Professor at the National Defence College, Stockholm, Sweden, and Visiting Professor at the Royal Military College of Science, Shrivenham, England. He is actively involved in the development and implementation of societal dynamics models of military, political, economic, and other processes for the modeling and analysis of low intensity conflict, peace and humanitarian operations, and related areas. He has published several textbooks, including The Military Landscape: Mathematical Models of Combat for which he was the co-author, and is the senior editor for several international conference proceedings. Dr. Woodcock was an I.B.M. fellow at the University of Warwick Mathematics Institute in England and at I.B.M. Research, Yorktown Heights, New York; a Fulbright Fellow and Research Associate in Biology at Yale University; an Assistant Professor of Biology at Williams College; and a visiting Scholar on sabbatical leave at Stanford University. He has a Ph.D. in Biology and an M.Sc in Biophysics from the University of East Anglia in England, and a B.Sc. (with honours) in Physics from Exeter University in England. He is a Full Member of Sigma Xi.

James E. Heath is the Army's Senior Intelligence and Technical Advisor for Information Operations (IO), Land Information Warfare Activity, Fort Belvoir, Virginia. He is recognized as the Army's leading technical authority on intelligence and information technologies for transnational and asymmetric threats. Multi-dimensional visualizations, predictive analysis, course-of-action analysis (COAA), and non-kinetic IO solutions are his current areas of interest. He was responsible for the creation of the Army Intelligence Command's (INSCOM) Information Dominance Center and serves as a technical advisor to the House Armed Services Committee on a Information Dominance technologies. He previously created the Focused Intelligence initiative within United States Forces Korea and helped create the Army's Battlefield Visualization program. While serving as the chief scientist for the Joint Precision Strike Program he was awarded the Army's Research and Development Award. He received his Ph.D. from the Department of Electrical Engineering at the University of New Mexico. His dissertation was on the "Discovery of Strong Coupling

Between Lattice-Band Carriers and Impurity-Band Carriers." He has a B.S.E.E. from the University of Washington and holds patents in infrared sensor technology.

INTRODUCTION TO INFORMATION OPERATIONS

Information operations as defined in the Joint Publication 3-13 of the Joint Staff (1998) are aimed at influencing the information and information systems of an adversary and defending one's own information and information systems. Such operations require the continuous and close integration of offensive and defensive activities, the design, integration, and interaction of command and control procedures with supporting intelligence, and may involve public and civil affairs-related actions (Figures 1 and 2). The following section provides a summary of the information on Information Operations contained in the United States Joint Staff Joint Publication 3-13 as an overview to the nature of information operations. This is followed by a description of the concept of Perceptual and Knowledge Landscapes and how these entities can serve as a metaphor for activities associated with information operations. This will set the scene for a brief review of the capabilities of the Information Dominance Centre being developed for the United States Army Land Information Warfare Activity.

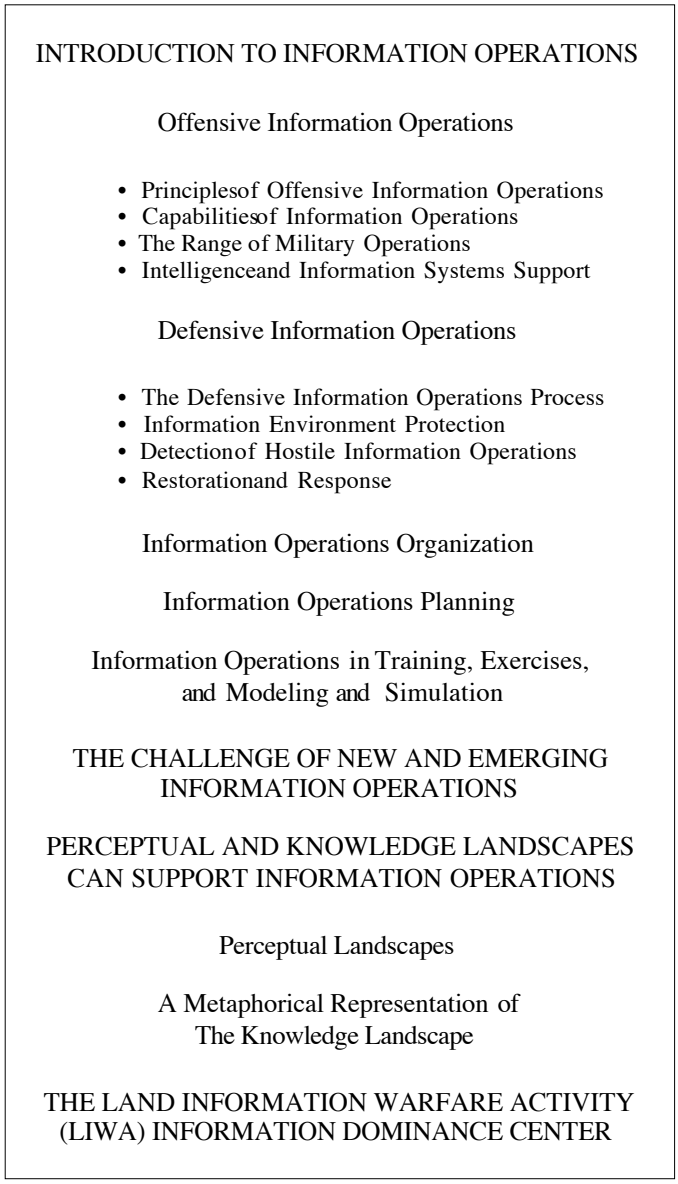

Figure 1: Information Operations in support of Civil-Military Interactions.

Offensive information operations involve the use of supporting information and intelligence capabilities and assets to influence adversarial decision-makers and to achieve specific objectives and may be most effective during he initial stages of an emerging crisis. Defensive information operations are aimed at protecting and defending friendly information assets through such activities as information assurance, operations security (OPSEC), physical security, counter-deception, electronic warfare, and special information operations. Information operations should be supported by a function information operations cell that can be responsive to a wide range of planning and operational circumstances and should be involved in all joint military operations. Planning for information operations must start at the earliest state of a joint force campaign and can involve both deliberate and crisis response activities.

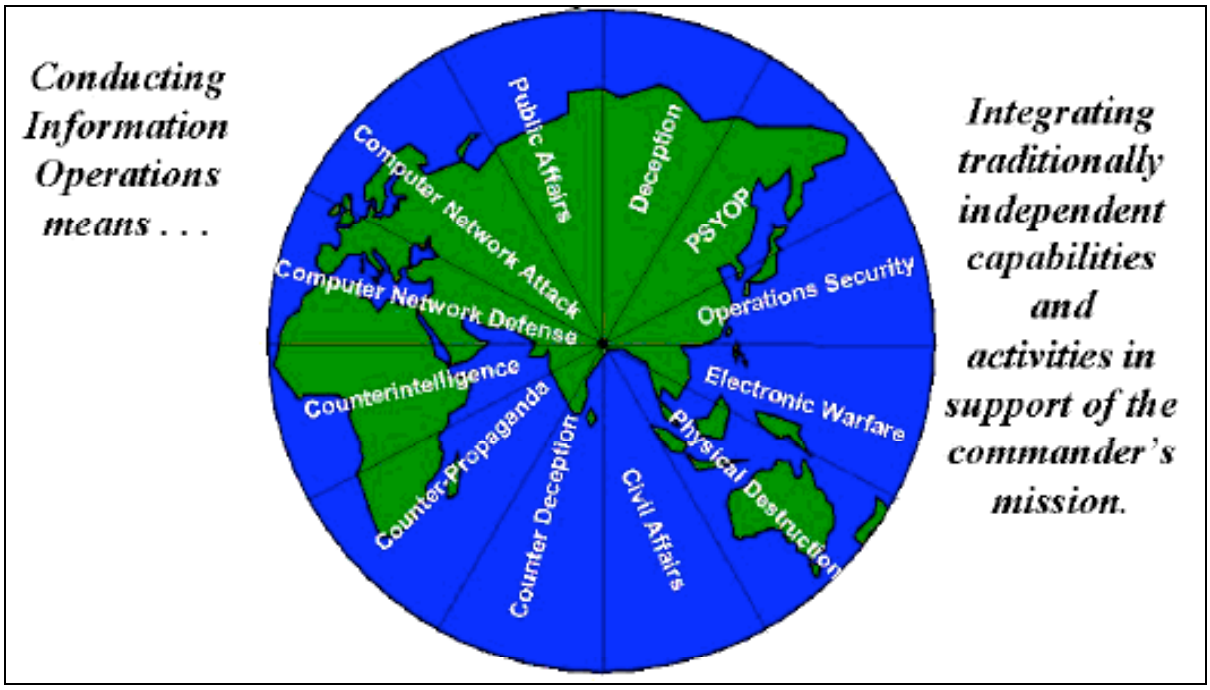

Figure 2: Information operations capabilities and related areas.

OFFENSIVE INFORMATION OPERATIONS

Offensive information operations are aimed at achieving advantage to United States forces across the range of military operations at every level of warfare.

PRINCIPLES OF OFFENSIVE INFORMATION OPERATIONS

As specified in the United States Joint Publication 3-13, Offensive Information Operations are "conducted across the range of military operations at every level of war to achieve mission objectives" [p II-1] The principles of information operations include the following:

- The human decision-maker is the intended target of information operation activities.
- Information operations targets and objectives and indicators of success should be identified clearly. Such operations can involve activities ranging from peace- to war-time activities.
- The selected information operations capabilities must match United States objectives and be appropriate to the task at hand.
- Information operations must be integrated, coordinated, and de-conflicted with all aspects of an overall military operation.

- Successful attack on the information and information systems of an adversary necessitates undertaking at least the following actions.

  > Development of an understanding of adversarial perspectives and its vulnerability to information operations attack.

  > Establishment of clear information operations objectives.

  > Identification of the value, use, information flow, and vulnerabilities of information systems.

  > Identification of targets and the most effective capabilities to influence those targets.

  > Estimate the impact of specific information operations on identified targets.

  > Obtain the necessary permission to employ information operations.

  > Identify methods for information operations impact assessment.

  > Undertake the planned information operations and evaluate the outcome with the aid of identified indicators and impact assessment methods.

CAPABILITIES OF INFORMATION OPERATIONS

Information operations involve the integrated use of many different types of capabilities including, but not limited to the following.

- *Operations security (OPSEC)* which is aimed at developing a good understanding of adversarial decision-making capabilities, denying critical information to an adversary, and slowing the adversaries decision cycle time.

- *Psychological operations (PSYOP)* are intended to influence adversarial emotions, reasoning, and eventually the behavior of foreign governments by providing selected information by many different means including personal contacts, media broadcasts, and the local use of loudspeakers.

- *Military deception activities* depend upon intelligence operations and involve the use of methods to mislead the thinking of an adversary and to create inaccurate impressions about the intentions, and capabilities of friendly forces , to misappropriate adversarial collection assets, and to create situations where adversarial forces are not deployed to maximal advantage.

- *Electronic warfare (EW) activities* can involve electronic attack, electronic protection, and electronic warfare support aimed at adversarial entities.

- *Physical attack and destruction* involves actions aimed at destroying particular targets.

- *Computer network attacks (CNA)* can involve the use of specialized software and other facilities to disable or destroy the computer facilities of an adversary.

- *Public affairs activities* are aimed at providing the public with a flow of timely and accurate information in order to create an awareness of military goals and of events that will influence the civilian sector.
- *Civil affairs activities* involve military actions that establish, maintain, influence, or exploit the relations between civil authorities, both governmental and non-governmental and the civilian population in order to facilitate military operations and support the achievement of operational objectives in friendly, hostile, or neutral environments. Civil affairs and PSYOPS are mutually-supportive during civil-military operations (CMO). During military operations other than war (MOOTW) such actions can be aimed at gaining support for a host nation and to reduce the destabilizing impact of hostile entities, for example.

THE RANGE OF MILITARY OPERATIONS

Offensive information operations can be undertaken across the range of military operations from peacetime to war and involve tactical, operational, and strategic components (Figure 3). An initial goal of information operations is aimed at maintaining peaceful conditions by defusing crisis situations and deterring conflict between potential adversaries. Under those circumstances where such preventative measured do not succeed, information operations can be applied to meet specific military objectives to counter the actions of an adversary.

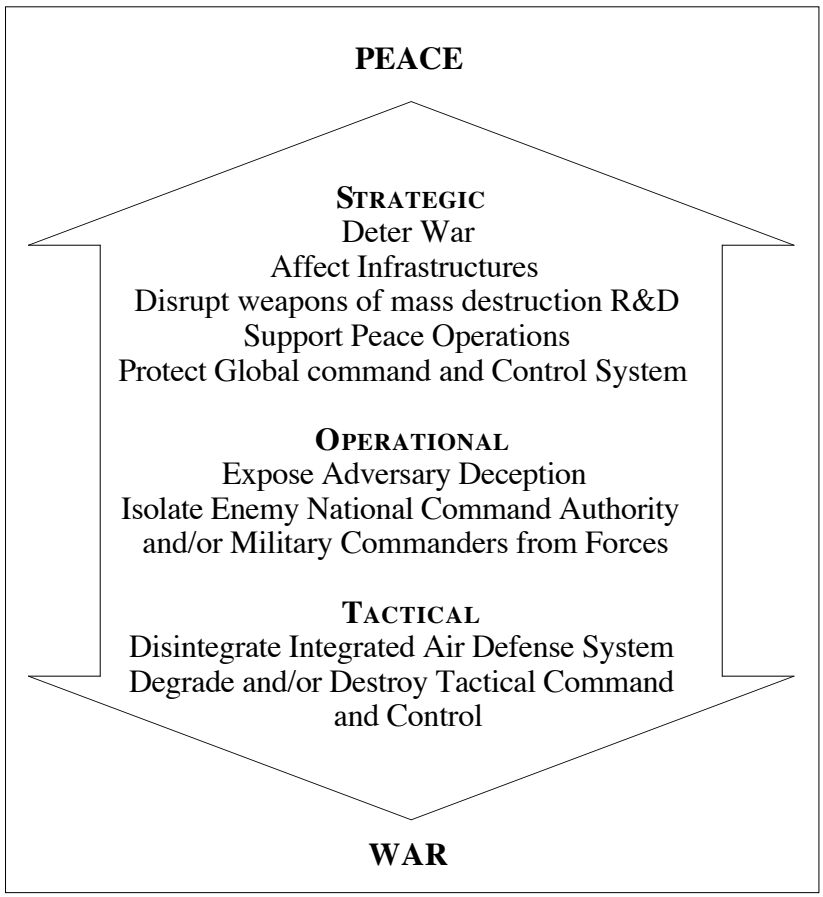

Figure 3: Examples of Information Operations Objectives (redrawn after: Joint Publication 3-13).

- *Military operations other than war (MOOTW)* involve the use of military capabilities in situations that are short of actual combat in such areas as deterring war, responding to crises, resolving conflict, and promoting peace by such actions as humanitarian assistance in conjunction with a peace enforcement operation.

- *Wartime operations* can involve activities at the strategic, operational, and tactical levels (Figure 3).

  > Strategic operations are normally directed by the National Command Authority (NCA) in coordination with the Department of Defense and other organizations and agencies. Such operations can deter crises and end hostilities by engaging adversary or potential adversary leadership or used to attack strategic targets while reducing the devastating effect of conventional military operations.

  > Operational activities can be undertaken within an area of responsibility (AOR) and will involve the use of military forces in order to achieve strategic objectives by focusing on the AOR of an adversary or potential adversary.

> Tactical activities are normally undertaken by a service or functional entity commander and are aimed at denying, disrupting, destroying, or control the adversarial use of information and information operations.

INTELLIGENCE AND INFORMATION SYSTEMS SUPPORT

Intelligence operations require dedicated intelligence support for their success and potential intelligence sources should be identified and activated as early as possible in the development of information operations. This will necessitate establishment of highly functional links between J-2 (Operations) and J-2 (Intelligence) entities (Figure 4) in order to provide necessary information operational support for a required Joint Campaign Plan. Intelligence collection can involve open sources such as the media, commercial contacts, academia, and local contacts as well as classified sources. Intelligence preparation of the battlefield involves the development of knowledge of the use by an adversary of information and information systems, the nature and use of adversarial decision-making processes, necessary political, economic, social, cultural influences, and in-depth biographical information of key adversarial leaders, decision-makers, and their advisors.

Guided by national strategic and other considerations, information operations personnel can use the intelligence products to develop a strategic framework for an operation. intelligence support can assist in the identification of adversarial decision processes and assist in the definition of the intent or mission for a Joint Force Commander. Additional intelligence support can serve to define the information operations environment and to develop objectives for the force commander. Identification of adversarial vulnerabilities can lead to the definition of tasks and sub-tasks that have to be undertaken during the operation. Intelligence input can serve to identify access opportunities to adversarial entities and assist in the definition of targets and or means for achieving particular goals. Such input and also support the production of measures of effectiveness in order to provide adequate assessment of the impact of particular information operations.

DEFENSIVE INFORMATION OPERATIONS

Defensive information operations ensure the protection and defence of information and information systems and such activities include protection of the information environment, the detection of attacks, the restoration of capabilities, and the response to an attack.

THE DEFENSIVE INFORMATION OPERATIONS PROCESS

The defensive information operations process is illustrated in Figure 5. Detection of an attack or the potential for an attack on a protected information environment can involve an assessment of the nature and severity of such attack, the reasons for the attack, and

identification of the actors responsible for the attack. These actors could include civil, criminal, military, informational, diplomatic, or economic entities. Subsequent analysis might reveal the intent of the actors. Such information could lead to the development and execution of a response aimed at influencing the perception of the actors and the deterrence of further attacks on the protected information environment.

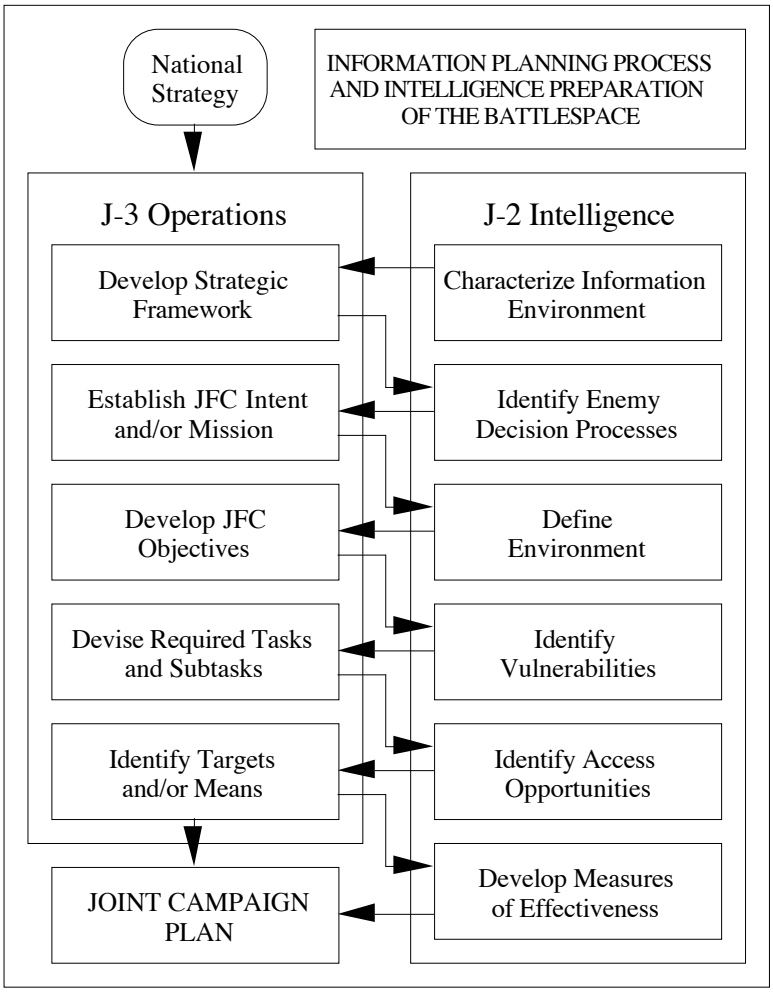

Figure 4: Information operations planning process and the intelligence preparation of the battlespace (redrawn after: Joint Publication 3-13).

- *Operations Security (OPSEC)* is a process that can be applied to any operation or activity and is involved in the identification and study of military operations in order to determine which activities and information elements could be observed by an adversarial intelligence system.

- *Electronic Warfare (EW)* can contribute to the protection and defence of information and information systems by changing call signs or words and managing broadcast frequencies, for example.

- *Education, training, and awareness* of joint force systems users, administrators, and administrators can alert individuals to the need to adhere to protective measures, to develop protective policies and procedures, and

develop the skills needed to operate while reducing joint force information vulnerabilities.

- *Intelligence support* can provide identification of potential or actual information operations threats, support the carrying out of threat assessments, and the development of options to manage risks from hostile actions. Such threats can involve insiders and authorized users, criminals and organized crime, terrorists, hackers, industrial espionage, and foreign entities (Figure 6).

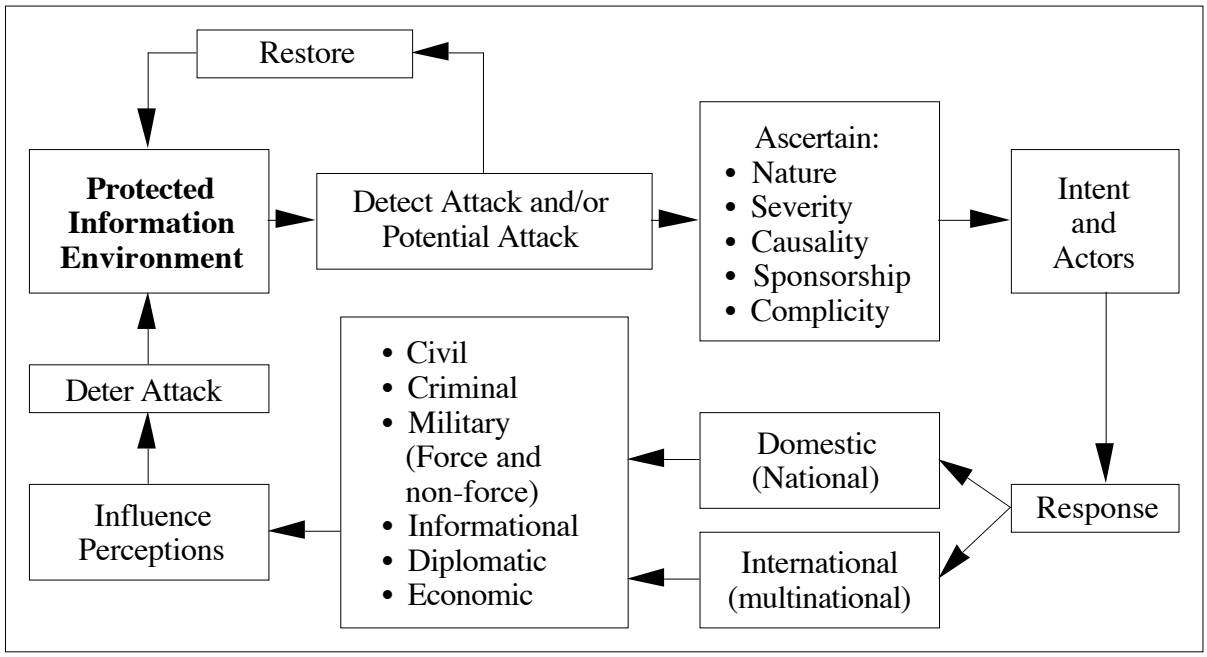

Figure 5: The Defensive Information Operations Process (redrawn after: Joint Publication 3-13).

- *Counter-deception* can reduce the impact of hostile information operations by identifying and acting against hostile entities.

- *Counter-propaganda* can serve to identify and act against adversarial actions aimed at influencing friendly civilian and military entities.

- *Counter-intelligence* actions protect and defend against espionage, sabotage, and/or terrorist activities.

- *Public Affairs actions* are involved in the provision of factual information in order to counter the impact of hostile propaganda.

INFORMATION ENVIRONMENT PROTECTION

Protection of information environments applies to all information media or form, including hard copy, electronic, magnetic, video, imagery, voice, telegraph, computer, and human.

Such protection involves determining what to protect, and the methods to be used in safeguarding identified information and information systems (Figure 7). This necessitates the development of policies and procedures and the use of appropriate technical and other facilities for vulnerability analysis and assessment and information protection.

DETECTION OF HOSTILE INFORMATION OPERATIONS

The timely detection of hostile information operations permits friendly forces to reduce the impact of such attacks and to restore initial system capabilities. Such detection necessitates the identification of potential or actual adversarial capabilities, including electronic warfare and military deception, and the development and use of appropriate intelligence capabilities. Intelligence can provide warning of hostile capabilities. Close coordination is needed between intelligence; counter-intelligence; law enforcement; and systems developers, providers, administrators, and users to permit the timely sharing of appropriate information related to hostile actions. Indications and Warning (I&W) involves actions that can alert appropriate individuals to the level of threat posed by particular entities and to potential or actual information warfare attacks on friendly military and civilian entities (Figure 8).

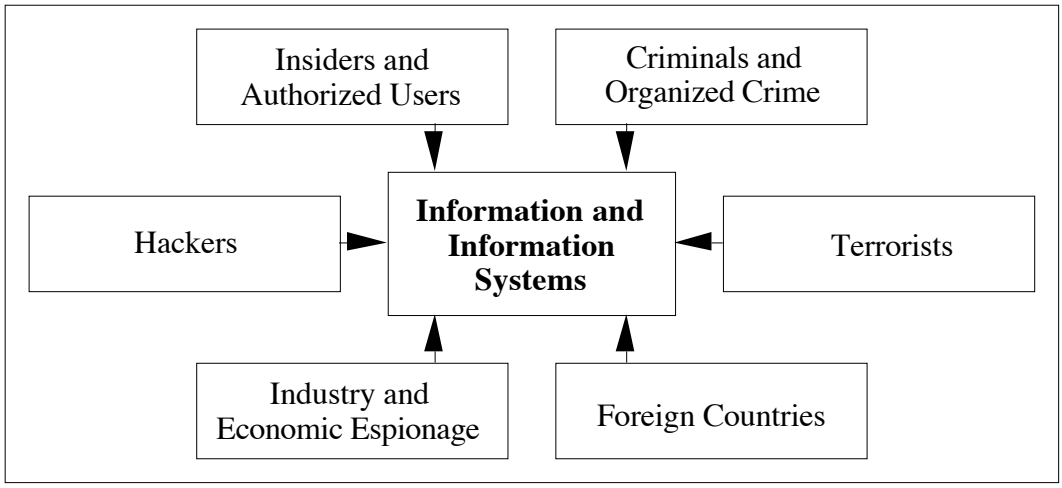

Figure 6: Growing threats to information and information systems are created my many different types of entity (redrawn after: Joint Publication 3-13).

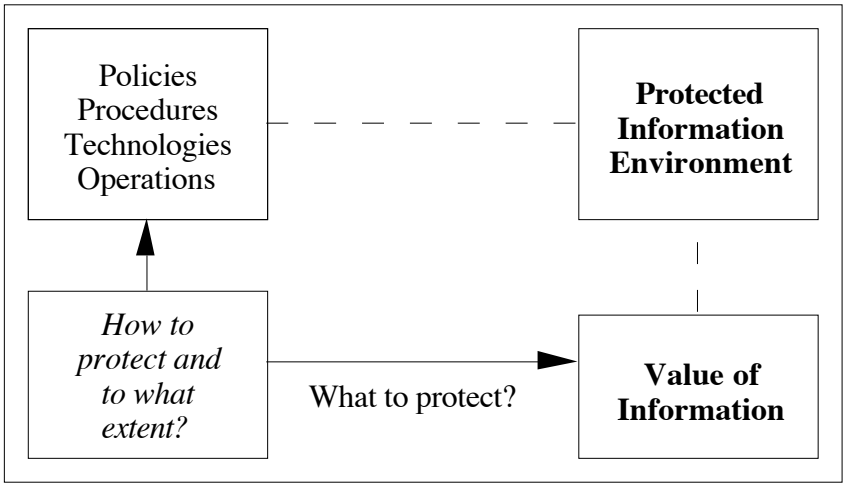

Figure 7: Information environment protection (redrawn after: Joint Publication 3-13).

RESTORATION AND RESPONSE

The restoration of capabilities after an information warfare attack often occurs on the basis of the importance of the target and can be facilitated by back-up facilities and other means of information transfer. Efforts are being made to incorporate automatic restoration facilities and redundant features that facilitate recovery from such attacks. Automatic intrusion facilities provide enhanced awareness of information systems to systems managers and administrators that can be used to terminate hostile access and even to alert law enforcement and other appropriate individuals. Of particular importance are Computer Emergency Response Teams (CERTs) which may be deployed to assist the restoration of capabilities in remote locations. Technical restoration can often be provided from other locations. A post-attack analysis can serve to identify the scope of the damage, the nature of the vulnerabilities that permitted the attack to take place, and appropriate improvements in security aimed at preventing further hostile actions from occurring.

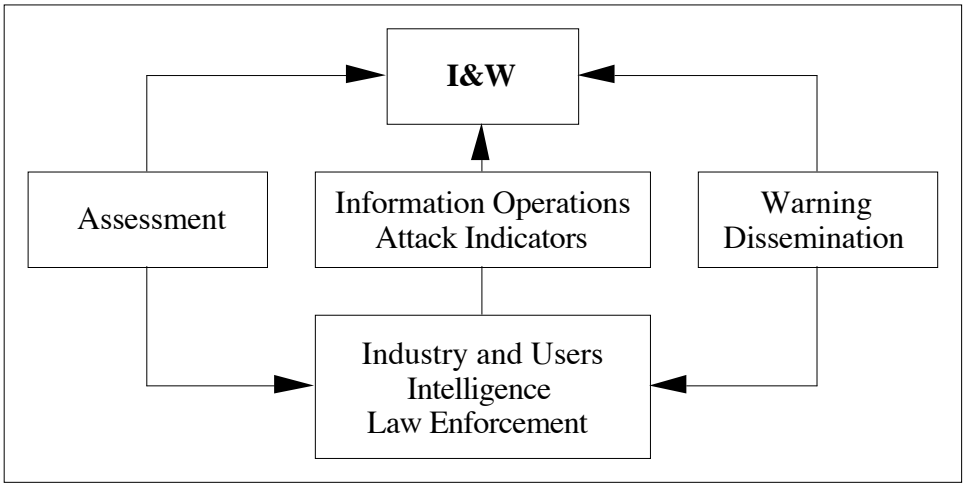

Figure 8: Indications and Warning in support of information operations provide alerts to hostile actions (redrawn after: Joint Publication 3-13).

INFORMATION OPERATIONS ORGANIZATION

The use of a fully functional Information Operations cell is critical to successful information operations. Such a cell would be formed with representatives from staff elements components, and supporting agencies and be involved in merging capabilities and related activities into a synergistic operational plan. The staffing of a typical joint Information Operations Cell is illustrated in Figure 9 and the functions of the information operations officer are shown in Figure 10.

- *The Operations Officer (J-3)* would normally be assigned by the joint staff who would ensure that the information operations were implemented in response to the guidance from the Joint Force Commander.

- *The Intelligence Directorate (J-2)* representative coordinates collection and analytic support for intelligence operations.

- *The Logistics Directorate (J-4)* representative coordinates and integrated logistics considerations for information operations.

- *The Plans Directorate (J-5)* representative integrates information operations into the overall planning process.

- *The Command, Control, Communications, and Computers directorate (J-6)* representative acts to coordinate the actions of information system-related individuals and to minimize the impact of offensive information operations.

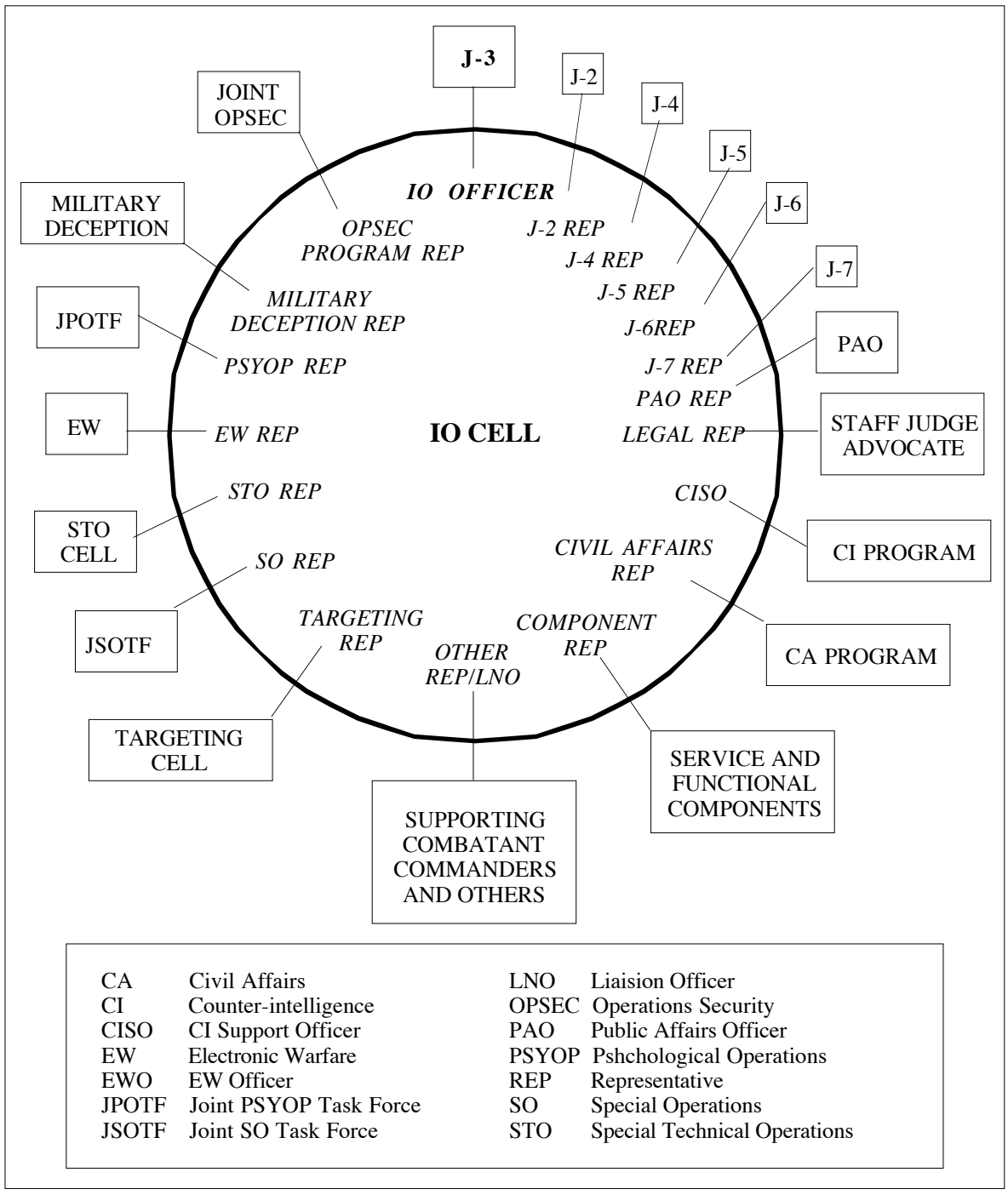

Figure 9: Typical staffing for a Joint Information Operations Cell (redrawn after: Joint Publication 3-13).

- *The Operational Plan and Interoperability Directorate (J-7)* representative integrates information operations into exercise and modeling and simulation.

- *The PSYOP* representative is involved in the integration, de-conflicting, and synchronization of psychological operations with in-theater and other entities.

_

- *The EW* representative works closely with J-6 and other entities to de-conflict friendly information operations.

Functions of the Information Operations Officer

- Coordinating the overall information operation (IO) efforts for the Joint Force Commander.
- Coordinating IO issues within the joint staff and with component staffs.
- Coordination of offensive and defensive IO.
- Establishing IO priorities to accomplish planned objectives.
- Determining the availability of IO resources to carry out IO plans.
- Recommending tasking to the J-3for joint organizations, staffs, and elements.
- Serving as the primary "advocate" for IO targets nominated for attack.
- Coordinating the planning and execution of IO between appropriate force elements.
- Coordinating intelligence and assessment support for IO.
- Coordinating IO inputs from joint centers and agencies.
- Coordinating liaison with the Joint Command and control Warfare Center, Joint Warfare Analysis Center, and other joint centers.

Figure 10: The functions of the information officer (after: Joint Publication 3-13).

- *The OPSEC* representative is involved with the J-6 representative in coordination of joint force command OPSEC actions.

- *The Military Deception* representative is involved in coordinating joint planning for military deception.

- *The Special Technical Operations* representative coordinates Joint Warfare Analysis Center (JWAC) support and may coordinate other support with the aid of the Planning and Decision Aid System.

- *The Counter-intelligence Support* representative is involved in coordinating information operations and counter-intelligence activities.

- *The Public Affairs* representative is involved in coordinating and de-conflicting public affairs activities.

- *The Legal/staff Judge Advocate* representative provides advice to planners in order to ensure that information operations comply with both domestic and international law.

- *The Civil Affairs* representative is involved in ensuring a consistency with all civil affairs activities in support of information operations.

- *The Targeting* representative represents and coordinates the actions of the entities involved in information operations targeting.

- The Other Organizational representatives and liaison officers provide links to such other organizations such as the united States Space Command, The

Defense information Systems Agency, the National security Agency, and Intelligence Agencies .

INFORMATION OPERATIONS PLANNING

Planning for information operations can take place under both deliberate and crisis conditions and must include the employment of all available information operations resources, including joint, Service, interagency, and multi-national. The fundamentals of campaign planning also apply to the development of plans for information operations (Figure 11). The establishment of subordinate entities and command relationships is critical to successful information operations in order to achieve unity of effort. Key to such success will be the early establishment of an information operations planning cell. Planning should commence at the earliest stage, and under ideal conditions, peacetime planning could provide the basis for subsequent information operations under either wartime conditions, or in support of MOOTW activities. Planning activities must include risk analysis of compromise, hostile reprisals, collateral damage, escalation of hostilities, and other factors.

Fundamentals of Campaign Plans

- Provide broad strategic concepts of operations and sustainment for achieving multi-national national, and theatre strategic onjectives.
- Provide an orderly schedule of decisions.
- Achieve unity of effort with air, land, sea, space,and special operations forces in conjunction with interagency, non-governmental, or private-voluntary organizations or United Nations or other multi-national forces as required.
- Incorporate the combatant commander's strategic intent and operational focus.
- Identify any special forces or capabilities the enemy has in the area.
- Identify enemy strategic and operational centers of gravity and provide guidance to subordinates for defeating them.
- Identify friendly strategic and operational centers of gravity and provide guidance to subordinates for protecting them.
- Sequence a series of related major joint operations conducted sinultaneously in depth.
- Establish the organization of subordinate forces and designate command relationships.
- Serve as the basis for subordiante planning and clearly define what constitutes success, including conflict termination objectives and potential post-hostilities activities.
- Provide strategic direction, operational focus, and major tasks, objectives, and concepts to subordinates.
- Provide direction for the employment of nuclear weapons as required and authorized by the National Command Authorities.

Figure 11: The fundamental activities associated with campaign planning (after: Joint Publication 3-13).

Coordination of information operations necessitates clear national strategic guidance in order to ensure that these operations support national objectives. Combatant commanders can use such guidance to subordinate entities for the planning and execution of information operations. In general, information operations will need to be supported by the long-term

development of intelligence in order to prepare the battle space for operational activity. In peacetime, information operations may be a principal way to achieve required objectives, and success in such operations requires the coherent integration of all available capabilities.

Information operations planning involves the identification of vulnerabilities of adversarial forces and the description of activities aimed at their exploitation in order to achieve the objective of the force commander. These planning activities will require access to Service, joint, and interagency information operations capabilities available to the force commander for planning purposes. Under some cases, authority to release and execute particular types of information operations may be required. The identification of hostile centers of gravity and the provision of guidance for defeating such centers and the corresponding identification of friendly force centers of gravity and the provision of guidance for their protection are fundamental aspects of the information operations planning process.

The information operations cell, described above, serves as the focal point for all information operations planning activities. The cell must be active in exchanging information with members of the cell and focus on the integration and de-confliction of information capabilities in order to facilitate the accomplishment of mission objectives. These activities should be undertaken continuously in order to permit the flexible and adaptable use of information operations facilities for mission support. In particular, information operations should be developed to support the overall operational planning of a joint force commander and take place simultaneously with operation planning. Guidance to operational planners is provided in the Joint Operations Execution and Planning System (JOPES) documentation.

Information operations planning can support both deliberative and crisis action situations.

- *In the Deliberative Planning Process*, information operations planning is an integral part of JOPES planning at the operational level. The general flow of deliberative planning activities are illustrated in Figure 12, and this scheme can be adapted for particular types of operation. However, when information operations planning is performed below the level of the combatant commander, it is of critical importance to inform the higher command level informed.

- *In the Crisis Action Planning Process*, activities occur in a compressed time interval, and planning coordination is even more important than in the case of deliberative planning. The general flow of crisis planning activities, which are shown in Figure 13, can be adapted to suit particular circumstances.

INFORMATION OPERATIONS IN TRAINING, EXERCISES, AND MODELING AND SIMULATION

Providing adequate training is of critical importance in to assuring the success of information operations. Such training should build upon the peace time information operations experiences and on appropriate background in crisis deterrence and conflict resolution. The fundamental considerations guiding exercise planning activities for information operations

are shown in Figure 14. Offensive information operations training should be provided both to individuals and organizations and demonstrate the integration of all available and potentially available facilities. Defensive information operations should also involve use of all appropriate available defensive facilities, including appropriate commercial and military assets.

Joint information operations-related exercises should involve appropriately complex and realistic environment in which realistic levels of synchronization, coordination, and de-confliction of information operations . Where suitable, military information-related activities should be related to those of multi-national forces, international organizations, and non-governmental organizations. These exercises should emphasize offensive information operations and the role of intelligence support and the protection and defense of information and information systems. Information operations should be incorporated into all planning and modeling and simulation in order to integrate such activities with modeling and simulation for other types of warfare. Modeling and simulation can also be used to assess and evaluate the impact of information operations on overall military capabilities.

THE CHALLENGE OF NEW AND EMERGING INFORMATION OPERATIONS

Joint Publication 3-13 serves as the foundation for addressing many of the new challenges within Information Operations. However, the key operational challenges are identifying Information Centers of Gravity, developing either non-kinetic or kinetic course of actions and defining the associated measurements of effectiveness. Identifying an Information Center of Gravity is an extremely complex process. This process is also very subjective since information operations are really about affecting how an opponent thinks, and the development of plans in relation to one's perception about a particular set of issues.

Information Operations Planning Related to Deliberate Planning

PLANNING PHASE	JOPES	IO CELL PLANNING ACTION	IO PLANNING OUTCOME
PHASE I	Initiation	Notify IO cell members of planning requirements	N/A
PHASE II	Concept Development		
Step 1	Mission Analysis	IO cell identifies information requirements needed for mission planning	Tasking to gather/obtain required information
Step 2	Planning Guidance	IO cell assists in development ofcombatant commander's IO planning guidance to support overall planning guidance	Combatant commander's planning guidance for IO
Step 3	Staff Estimates	IO cell supports development of intelligence, operations, and communications staff estimates	IO portion of staff estimates
Step 4	Commander's Estimate	IO cell assists in transforming staff estimates into the Commander's Estimate	IO portion of Commander's Estimate
Step 5	Combatant Commander's Concept	IO cell assists in the IO aspect of Combatant Commander's Concept as required	IO portion of Combatant Commander's Concept
Step 6	CJCS Concept Review	IO cell assists in the IO aspect of CJCS Concept Review as required	IO portion of operational concept approved by CJCS
PHASE III	Plan Development	IO celldevelops the complete IO plan and plans for each of the IO elements in coordination with appropriate staff sections, operational units, and supporting agencies	Draft offensive and defensive IO appendices
PHASE IV	Plan Review	IO cell modifies/refines plan as necessary	Approved offensive and defensive IO appendices
PHASE V	Supporting Plans	Subrdinate units and agencies prepare their own IO plans. IO cell coordinates/assists subordinate and supporting IO plan as necessary. Ensure the Time-Phased Force and Deployment Data (TPFDD) supports IO plan	Completed subordinate and supporting agencies' supporting plans. IO plan supported by TPFDD

Figure 12: Information operations planning related to deliberate planning (from: Joint Publication 3-13).

Information Operations Planning Related to Crisis Action Planning			
PLANNING PHASE	JOPES	IO CELL PLANNING ACTION	IO PLANNING OUTCOME
PHASE I	Situation Development	IO cell identifies planning information requirements as situation develops	Tasking to gather/obtain required information
PHASE II	Crisis Assessment	IO cell identifies information requirements needed for mission planning. IO cell assists in development of combatant commander's IO planning guidance to support operational planning guidance	IO planning guidance. Initial liaison with units and agencies that may participate in or support IO activities
PHASE III	Course of Action Development	IO cell supports development of intelligence, operations, and communications staff estimates	IO portion of staff estimates
PHASE IV	Course of Action Selection	IO cell assists in transforming staff estimates into the Commander's Estimate. IO cell assists in the IO aspect of Combatant Commander's Concept as required.	IO portion of overall plan approved through CJCS
PHASE V	Execution Planning	IO cell develops the complete IO plan and the plans for each of the IO elements in coordination with appropriate staff sections, operational units, and supporting agencies	Approved offensive and defensive appendicies with element tabs, completed supporting plans, and inclusion of IO requirements for the Time-Phased Force and Deployment Data (TFFDD)
PHASE VI	Execution	IO cell monitors IO operations and adapts IO objectives to support changing operational directives	IO objectives modified as necessary to support changing operational objectives

Figure 13: Information operations planning related to crisis action planning (from: Joint Publication 3-13).

The complexity associated with defining Information Centers of Gravity results from trying to understand relationships between individuals and groups and their associated variables. These one-to-many or many-to-one relationships are dynamic in nature thus, further complicating an accurate temporal understanding of the situation. Because these dynamic variables involve such things as political, economic, and social relationships, traditional military maps and symbology are often inadequate for accurately portraying the situation. In the following sections some new approaches and techniques for determining and displaying Information Centers of Gravity and their components will be discussed.

Once an adversary's Information Center of Gravity can be determined it must then be incorporated into the military commander's situational awareness picture to enable course-of-action planning. However, as discussed in the above this is very difficult when the situation does not involve a force-on-force problem. Similarly, how does one formulate a non-kinetic course-of-action and synchronize one's actions over very long time frames measured in months or years? Longer time frames associated with non-kinetic solutions are often required when associated with changing either an individual's or a group's perception. For an IO course-of-action to be effective one is really attempting to lengthen the opponent's capability to observe, orient, decide and act (OODA loop). In turn, this provides more time for the military commander to achieve a non-kinetic solution or to pick the time and place for a kinetic solution. In order to develop IO courses-of-action new techniques, such as Q-Analysis, (Woodcock and Heath, 1999, this volume) are required.

Traditional centers of gravity are based on physical relationships while Information Centers of Gravity are based on complex, ill-defined relationships. Therefore, being able to quantify an IO battle damage assessment or measurement of effectiveness is quite different since it does not necessary involve a physical change. These measurements of effectiveness require techniques that enable one to understand how to create changes within the adversary's decision cycle or alter one's perception about particular sets of issues. In the following section, techniques for understanding perceptual changes will be discussed. These techniques provide some insight into the difficulty associated with defining measurements of effectiveness for IO courses of actions.

Fundamental Information Operations
Exercise Planning Considerations

- Develop concrete, attainable IO objectives.
- Provide for sufficient IO actions to support exercise objectives.
- Create as realistic an IO exercise environment as possible.
- Assess and evaluste the employment of IO.
- Exercise both offensive and defensive IO using all the capabilities are available and compatible with the exercise scenario.
- Exercise intelligence support to IO.
- Use appropriate security measures to protect IO tactics, techniques, and procedures.
- Evaluate use of computer support products to plan and evaluate IO.
- Evaluate the use of simulations to fulfill some IO training objectives.

Figure 14: Fundamental planning considerations for information operations exercises.

INFORMATION OPERATIONS AND THE TRANSFORMATION OF DATA INTO KNOWLEDGE

The complexity of the societal environments within which information operations generally take place has provided severe challenges to conventional modeling and analysis methods and the associated processes of data collection and manipulation. New, non-traditional methods appear to be necessary to meet these challenges (Woodcock, 1995). Successful

information operations require an understanding of how data is transformed into knowledge and how internal world models of an external reality are created in the human brain. The new modeling approaches must provide insight into such processes and demonstrate how they could be modified by information operations. This section describes the phenomenon of perceptual ambiguity and outlines the nature of internal world models. The following section outlines how entities called Perceptual and Knowledge Landscapes can provide new types of insights to support Information Operations and other activities.

Internal models appear to play a critical role in the interactions that we make with the external world. Understanding the nature of these models as well as the causes and effects of perceptual ambiguity are key tasks to be faced by the Information Operator. Protection and modification of internal models and the decision-making processes that they support must be seen as the ultimate target of information operations. The ambiguity of perception creates both risk and opportunity. Risk occurs when two views of the same situation can lead to confrontation and conflict. Opportunity can occur when the reconciliation of different views can lead to greater understanding of the nature of a particular situation.

It can be argued that information is generated by considering data elements in the context of other elements. It also can be argued that perceptions can be generated when information is viewed in the context of other information. Similarly, cognition could result from the consideration of some perceptions in the context of other perceptions and knowledge can represent the contextual consideration of different cognitions. Belief can emerge from the integration of contextual knowledge. These activities involve essentially nested processes and can occur on many different time scales. Thus, data collection and storage may take place in times ranging from seconds to hours while the creation and modification of beliefs can take years, or even lifetimes.

PERCEPTUAL AMBIGUITY PROVIDES CLUES TO THE TRANSFORMATION OF DATA INTO KNOWLEDGE

Examination of the phenomenon of ambiguous visual perception can assist in the development of an understanding of the ways that data and information may be translated into knowledge. Everyday experience provides examples of perceptual ambiguity where sudden changes in perception and understanding can occur. The Necker cube (Figure 15) illustrates the phenomenon of sudden perceptual change created by perceptual ambiguity. As you view the illustration your perception appears to undergo a series of “jumps.” First the cube appears to be pointing out of the paper, then it appears to be pointing into the paper, for example. There is at least suggestive evidence that such perceptual changes may occur in the minds of individuals as they think about complex societal activities.

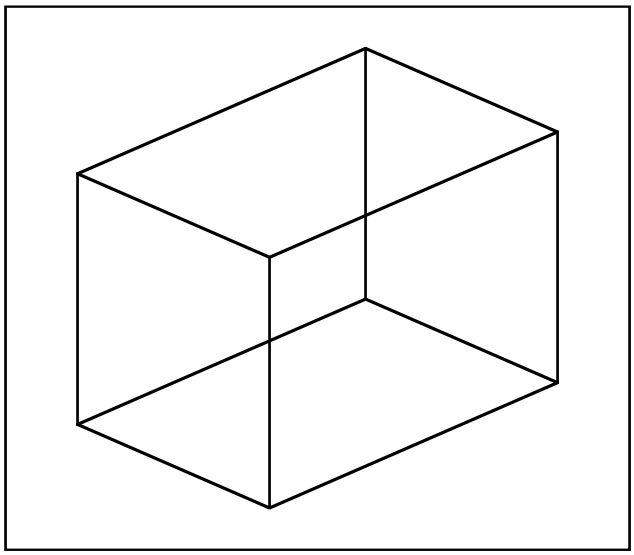

Figure 15: The visually ambiguous nature of the Necker cube provides an illustration of the creation of information from data and the creation of perceptions from viewing information in the context of other information.

Let us examine what is happening as you view the cube. First visual sensory cells detect the individual small line segments of the diagram. Points (which are zero-dimensional entities) viewed in the context of other points provide information on the existence of lines (which are one-dimensional entities). Lines viewed in the context of other lines generate the perception of surfaces, which are two-dimensional entities. Surfaces viewed in the context of other surfaces generate the perception of volume. When focusing on one corner of the cube creates the perception that the cube appears to be pointing of the paper. However, when that point is viewed in the contest of the neighboring point, the cube appears to jump. The viewing of one perception in the context of another perception and the cognitions that this generates provides you with knowledge of the overall behavior of the cube. At a future time, when someone mentions the Necker cube, you should be able to remember the experience of viewing the transformation and even recapitulate the jumping behavior in your "minds eye," as it were.

INTERNAL MODELS CAN REPRESENT EXTERNAL REALITY

The processes of perception, cognition, and knowledge development lead to the creation of internal representations of external entities and behavior (Woodcock, 1995). As mentioned above, understanding the nature of such processes can provide important insights into the ways that the human mind uses data and information and how this could be modified by information operations. The processes by which sensor inputs are transformed into knowledge and understanding has been described and modeled by many individuals. As an interesting historical example, Plato in *The Republic* provides a scheme for representing the different levels of description of entities. As outlined below the scheme provides insights which can provide useful insights for modern-day activities (Figure 16). The Platonic scheme considers that representations of the world can be divided into visible and intelligible components (Grube 1978). The process is described in terms of an upward journey from

mere sensory awareness to perfect and complete knowledge, which also involves an ascending scale of reality.

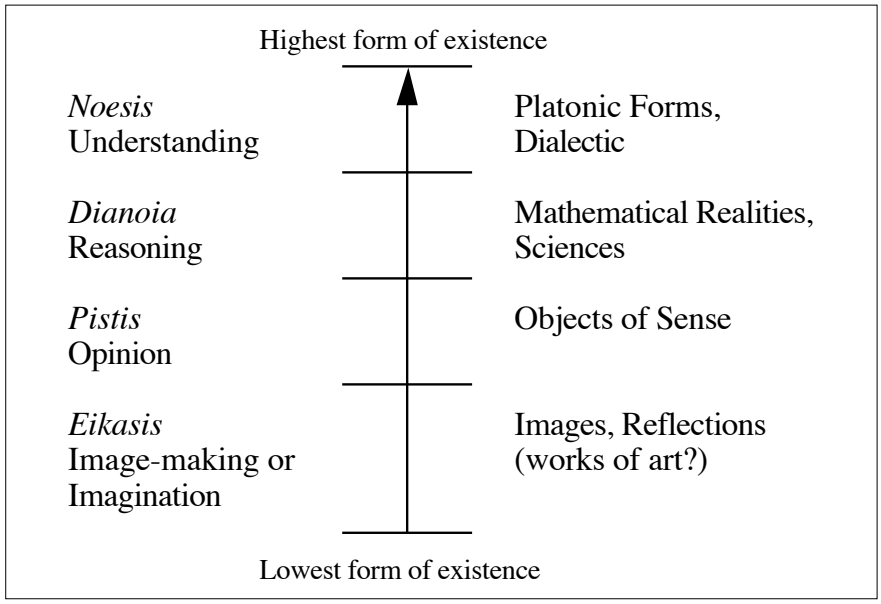

Figure 16: Graphical representation of Plato's description of world representations described as: *Noesis* (Understanding), *Dianoia* (Reasoning), *Pistis* (Opinion), and *Eikasis* (Image-making or Imagination). (Modified after: Grube, G.M.A. 1974. *Plato's Republic.* based on: Plato (428-7 to 347 B.C.), *The Republic*, *Book VI*; from Woodcock, 1995).

- *Image-making or Imagination* (Greek: *Eikasis*) is the lowest level of the scheme and is characterized as image-making or imagination and involves the formation of images, reflections of entities, and graphical representations of objects.

- *Opinion* (*Pistis*) is the second level of the scheme and involves the formation of models of the images, living creatures, plants, and manufactured entities generated at the initial level. In this case, selected attributes of these entities are used to form an abstracted representations of these entities.

- *Reasoning* (*Dianoia*) is the third level and consists of scientific or mathematical representations of the objects of sense that have been generated from consideration of the products of the first two levels. These representations can capture relationships between the entities and such relationships may be expresses as scientific rules.

- *Understanding* (*Noesis*) involves an idealized description of entities based on basic, geometric, properties of nature, something that Plato associated with the actions of the soul. This fourth level describes entities and relationships in terms of scientific laws and principles that capture some form of established knowledge of their nature and behavior.

The Platonic principles outlined above have provided the basis for generations of scientific and mathematical research and development. The development by Thom (1978) and Zeeman (1978) of a branch of mathematics called Catastrophe Theory can be considered to be in the Platonic tradition. The theory describes the behavior of systems in terms to idealized mathematical entities called catastrophe manifolds or landscapes (Poston and Stewart, 1978; Woodcock and Davis, 1978, and Woodcock and Poston, 1974). While it is not appropriate to give an exhaustive description of the theory in this paper, the next section will illustrate how the catastrophe landscape approach can provide models of perception and provide descriptions of the behavior of societal entities. Models based on catastrophe theory have been used to support the development of indicators and warnings (Woodcock, Cobb, and Langendorf, 1993) as well as information operations. Landscape models provide non-traditional ways to represent data, information, and perceptions. Such methods are needed to provide insights into the complicated and rapidly changing nature of on-going events that severely challenge more conventional modeling and analysis techniques.

PERCEPTUAL AND KNOWLEDGE LANDSCAPES CAN SUPPORT INFORMATION OPERATIONS

Information operations take place in complex environments involving the interactions of many different types of military and civilian entity. Understanding the nature of such environments and the inter-relationships between the entities is of obvious importance for planning and undertaking activities aimed at modifying behavior and achieving defined goals. A catastrophe theory-based modeling approach has been adopted to the analysis of threat assessments of notional intelligence data by military intelligence analysts (Woodcock, Cobb, and Langendorf, 1993, for example). Catastrophe theory can provide the basis of entities called perceptual landscapes that can illustrate the perceptual ambiguity associated with the Necker cube (Figure 15). This landscape shows how the cube can appear as an ambiguous or conflicting object and how sudden changes in perception can occur as the cube appears to jump into or out of the page under certain conditions (Figure 17).

PERCEPTUAL LANDSCAPES MODEL POLITICAL CONFLICT

It is possible to use the perceptual landscape to describe the conflicting perceptions a about the events that occurred recently in Kosovo. These events in Kosovo appear to be caused in part by the existence of entrenched conflicting perceptions. Such perceptual conflict can create the basis of misunderstanding that may lead to intransigence and to increasingly violent conflict. Thus, to the leadership in Belgrade, the ethnic Albanians in Kosovo were sub-humans that had to be purged and "ethnically-cleansed" and the Serbs in Kosovo the only humans with rights in the province. The ethnic Albanians obviously had a completely different perception of the situation and the ethnically Albanian KLA force undertook extensive military operations against the Serbian-led Yugoslavian army.

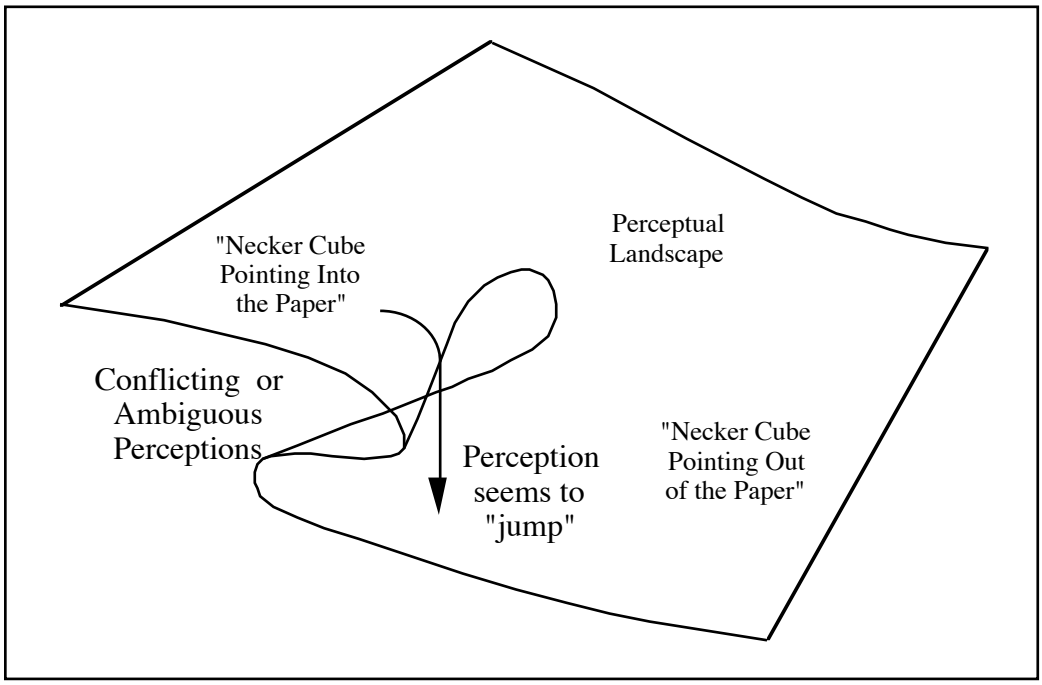

Figure 17: A perceptual landscape based on the Cusp catastrophe provides a geometric metaphor for the perceptual ambiguity of the Necker cube.

The ambiguity associated with the different perceptions of the ethnic Serbian and Albanian factions in Kosovo is illustrated with the aid of a perceptual landscape in Figure 18. Positions on the landscape are defined in terms of the levels of perceived ethnic Serbian and ethnic Albanian isolation. High levels of perceived isolation for both ethnic groups can create a politically polarized situation involving mistrust and hatred between the groups that can lead to conflict. In this case, the two groups are looking at obstensively the same world in completely different ways. This difference in perspective can be likened to the different ways that the Necker cube can be viewed. The perceptual jumps that occur as you view the cube can be likened to the dramatic changes in political perception as one looks at the situation in Kosovo first from the ethnic Serbian, and then from the ethnic Albanian viewpoint. Neither viewpoint is “wrong,” they are basically different due to the inherent perceptual polarity of the overall situation.

The perceptual landscape metaphor can provide a simple illustration of the causes of ethnic conflict in Kosovo and elsewhere. The landscape can also suggest methods for conflict resolution and prevention. In this case activities aimed at reducing the perception of isolation of the two ethnic groups can reduce the high level of political polarization and move them towards conditions of potential and ethnic coexistence. These activities could involve the use of external political, economic, military, and other resources to foster the establishment of societal conditions where at least some members of each minority could begin to work with external entities for their benefit, and that of other groups, for example. It is evident that the wide spectrum of information operations described earlier in this paper must play key roles in such processes.

KNOWLEDGE LANDSCAPES CAN CAPTURE POLITICAL AND MILITARY DATA AND INFORMATION

Landscapes based on catastrophe theory have also been used to describe the military conflict environment and to illustrate the impact of force strength and other parameters on conflict outcomes (Dockery and Woodcock, 1993). Knowledge of the military conflict environment includes information on the nature of military forces and their behavior when subjected to different political, military, combat, terrain, logistic, and other types of constraint . Historical knowledge associated with battles on actual battlefields can be used to guide the training of military personnel in order to produce an increased understanding of the nature of combat. Such information can also be embedded within a virtual environment in order to facilitate the study and analysis of military processes and to examine the impact of new types of technology, tactics, strategies, information warfare, and other properties on military performance and combat capability.

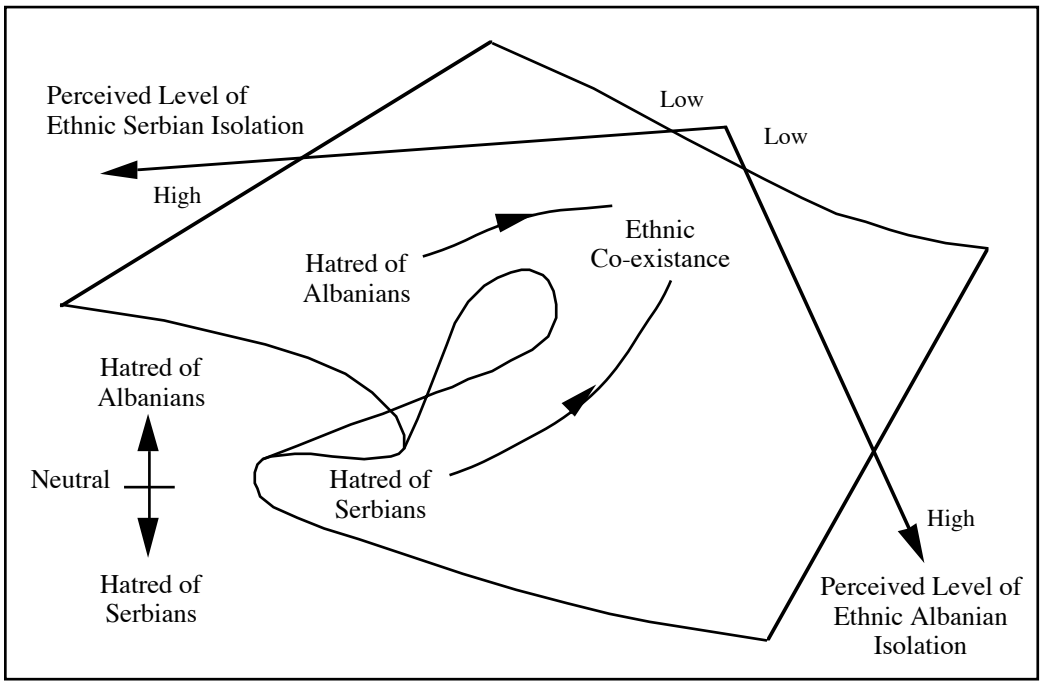

Figure 18: A perceptual political landscape can represent the extreme political polarization associated with conditions in Kosovo and suggest strategies for reducing that polarity.

Virtual military environments can be provided with entities that give a metaphorical representation of specified conceptual properties (Figure 19). Such entities could be tasked with performing particular types of activities within the virtual military environment. They could also be provided with an iconic representation that invokes such metaphorical constructs within the mind of the user. Indeed, computer-based agents or avatars have been represented as stylized human-like entities in some systems. Other metaphorical representations will surely appear in the very near future. Activities involved in the modeling and analysis of military and other types of societal behavior can generate knowledge that could support training and the guidance of future actions. The collection and integration of such knowledge can be used to construct metaphorical entities that Woodcock (1995) has called *Knowledge Landscapes* (Figure 20).

Knowledge Landscapes provide a metaphorical representation of the information contained in historical maps produced by early explorers. Regions that were either close to home or had been explored extensively were drawn in great, and hopefully accurate, detail. Areas that were poorly explored should have been represented less in detail. Unexplored areas were often described as an unknown land, a *terra incognito*. The heights of points on the knowledge landscape can represent the amount of knowledge that has been collected about a particular situation. Relatively well-known subject areas can be represented as peaks on a knowledge mainland. Isolated areas of knowledge, perhaps reflecting the emergence of new areas of study, can be represented by knowledge islands that are separated from the mainland.

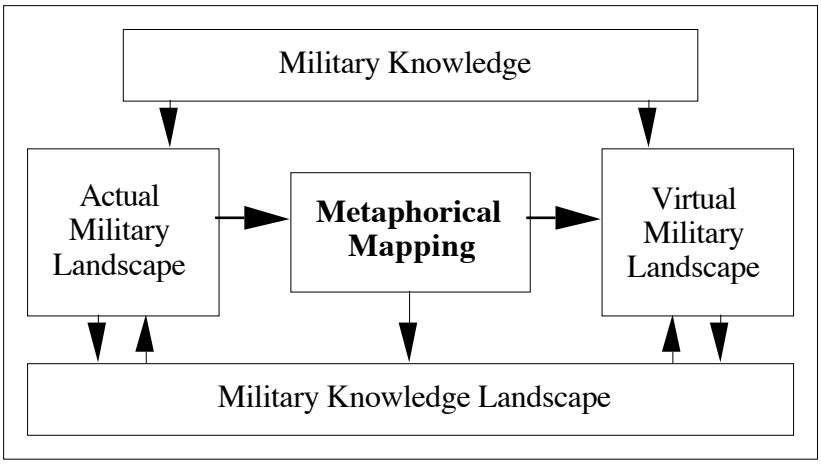

Figure 19: Military knowledge can be reflected in the nature of actual military landscapes and can be used to construct a virtual representation called the Military Knowledge Landscape by a process called metaphorical mapping (from: Woodcock, 1995).

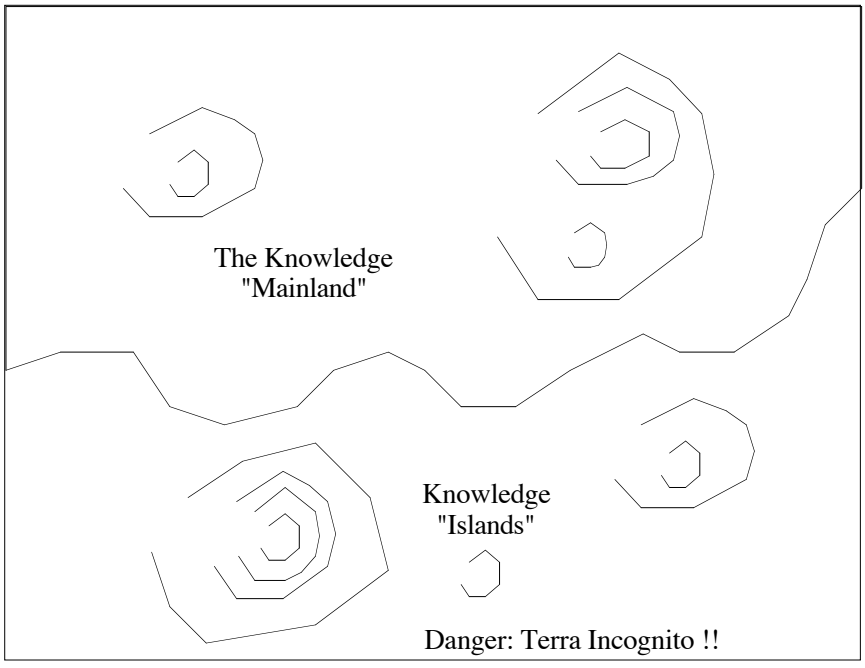

Figure 20: A geometric representation of the knowledge landscape (from: Woodcock, 1995).

Activities of pioneering scientists and mathematicians can be likened to the activities of early explorers involved surveying the geographical landscape. In the former case, the scientists are involved in actually constructing the knowledge landscape as well as in surveying the landscape in order to identify pathways that could be build to link apparently different areas of knowledge. One form of such a landscape could consist of a multi-dimensional space with each of the dimensions representing a particular aspect or property of the system or entity of interest. Development of a virtual reality-based, multi-dimensional, knowledge landscape could assist in the identification of areas where knowledge development activities should be undertaken. The final section of this paper describes how the non-traditional perceptual and knowledge landscape concepts have been realized during development of the Information Dominance Centre (IDC) at the US Army Intelligence and Security Command (INSCOM), Land Information Warfare Activity (LIWA).

THE LAND INFORMATION WARFARE ACTIVITY (LIWA) INFORMATION DOMINANCE CENTER

The Land Information Warfare Activity is embracing a number of technologies to facilitate the transition from split-based operations to virtual operations. LIWA's central facility, the Information Dominance Center (IDC), will simultaneously support many Field Support Teams (FST) distributed throughout the world communicating over whatever network topology is available (Figure 21). LIWA will maintain a truly collaborative distributed environment (i.e. collaborative virtual environment) to facilitate rapid situational awareness and centralized support to these external teams. Non-traditional techniques for harvesting huge amounts of both open source, such as that shown in Figure 22, and classified data, are needed to support information operations.

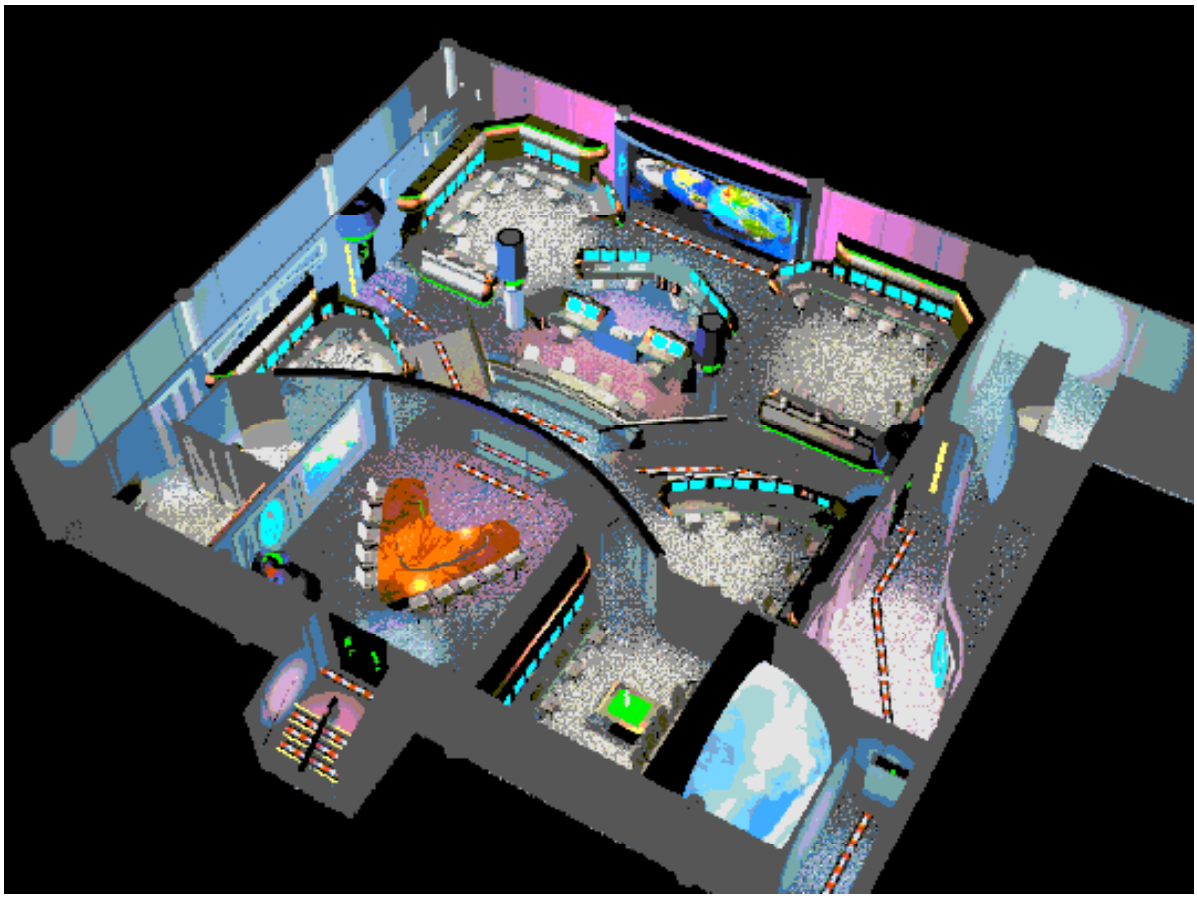

Figure 21: The Land Information Warfare Information Dominance Center.

Other non-traditional methods are needed to identify patterns and relationships and generate information on the nature of the environment from which the data was obtained. Figure 23 represents one of the many visualization techniques used within the IDC. Harvested information is organized by themes or issues using a landscape metaphor. In essence this provides the Perception or Knowledge landscapes described earlier. Figure 24 shows a screen capture from the IDC's video cataloging component, just one of many IDC open source harvesting tools.

The Information Dominance Center uses Asynchronous Transfer Mode (ATM) input to the desktop for extremely high local performance, as well as with high speed interconnects to other important DoD and open information sources. Field Support Teams and other remote sites will typically have multiple network connections including satellite and land based access. The collaborative virtual environment under development at LIWA encompasses the following capabilities.

Selections from the BiH TV news summary 14 April 1999 broadcast at [19:30]

* Heads of states and governments of the European Union met in Brussels in order to discuss resolving of the Kosovo crisis.

_

* UK Defence Minister Robertson said that former Bosnian Serbs General, Ratko Mladic, who has been indicted for war crimes, participates in ethnic cleansing in Kosovo.

* NATO concerned for security in the countries of the region after intrusion of Serbian troops in Albania.

* According to assessments of the Western Alliance, about 280.000 Kosovo Albanians roam around Kosovo wastelands.

* SFOR spokesperson Sheen Thompson said that Russian contingent in SFOR remains a part of BiH stabilisation forces.

Figure 22: Open-source text materials can provide inputs to non-traditional information extraction and knowledge development processes.

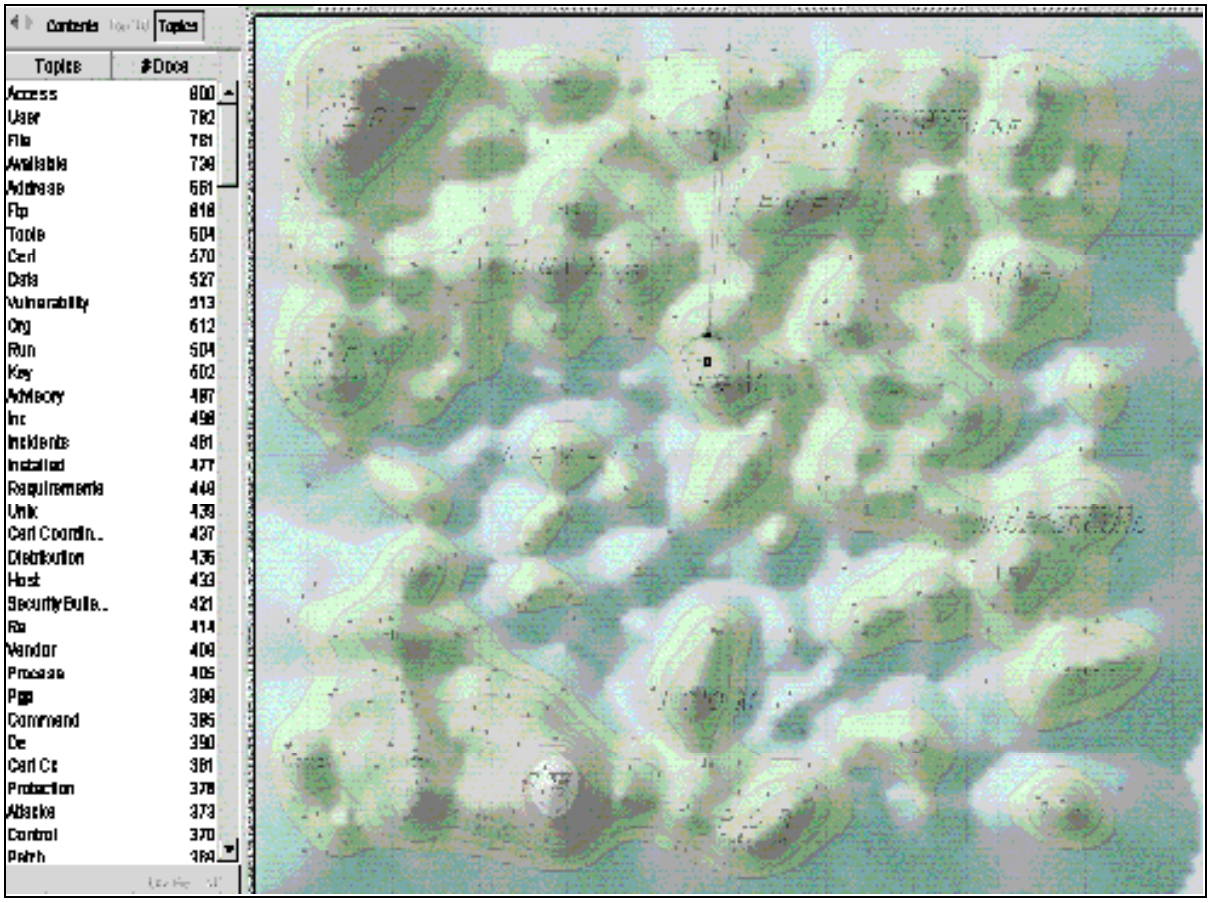

Figure 23: A knowledge landscape created by the analysis of open-source text materials can support information operations.

1. *Video / Audio:* Within the IDC, audio and video collaboration will be supported using MPEG-2 (for high quality broadcast of conferences or upper level command) and MPEG-1 (for small group workstation collaboration) facilities.

2. *Application Sharing and Shared Whiteboards:* Application Sharing involves infrastructure to facilitate multiple views of and control over a single application. Whiteboards, chat windows, etc., provide another way for users to share data. Most whiteboards allow drag and drop of images, and interactive graphic gesture creation.

3. *Data Sharing:* In many ways, the IDC maps more closely to conventional corporate data infrastructures in its use of standards based centralized data infrastructures. Shared Relational and Object Oriented Databases will provide the core integration support for implementing the IDC's overall functionality.

4. *Publish / Subscribe Event Distribution and Message Oriented Middleware:* Event services techniques involve the creation of channels for a number of event categories. Client applications register interest by subscribing to channels and are asynchronously notified whenever a Source application sends an event into the channel. Message Oriented Middleware (MOM) involves a centralized, reliable, message store provides the persistence necessary to implement this capability that can support loosely coupled applications, a capability that is critical to LIWA. MOM infrastructure will greatly simplify the implementation of the support applications for the Field Support Teams.

5. *Distributed Model-View-Controller (MVC) Infrastructure:* The IDC is developing a distributed Model-View-Controller (MVC) architecture for facilitating the development of tightly coupled applications. MVC, which is perhaps the most common architectural model used for developing event-based, shared-data applications, can be distributed with the aid of such commercial communications infrastructure tools as CORBA, DCOM, or Java Remote Method Invocation (RMI).

SUMMARY AND CONCLUSION

Information Operations in support of civil-military interactions is becoming increasingly more important as non-kinetic courses-of-action are required. Incorporating information operations into military operations up until now has been extremely difficult due to the lack of doctrine and operational or technological support. However, Joint Publication 3-13 of the Joint Staff has addressed the doctrinal requirements while innovative operational sites such as the Army's INSCOM Information Dominance Center are addressing the operational and technological needs. In fact, the IDC serves as a model for both the Department of Defense and a proposed virtual hearing room for Congress.

As the IDC and its supporting technologies mature, individuals will be able to freely enter, navigate, plan, and execute operations within perceptual and knowledge landscapes. This capability begins the transition from Information Dominance to Knowledge Dominance. The IDC is instantiating such entities as smart rooms, avatars, square pixel displays, polymorphic views, and other technologies for directly interacting in virtual domains. This will take us to the next paradigm of human-machine interaction within the multi-dimensional

spaces required for Information Operations. These activities must also involve the development and use of new techniques that create insights into the ways that data and information are transformed into knowledge. The understanding of the properties of knowledge-based internal world models that can emerge from these activities should provide the basis for new technologies to support information operations and their use in many activities including peace and humanitarian operations.

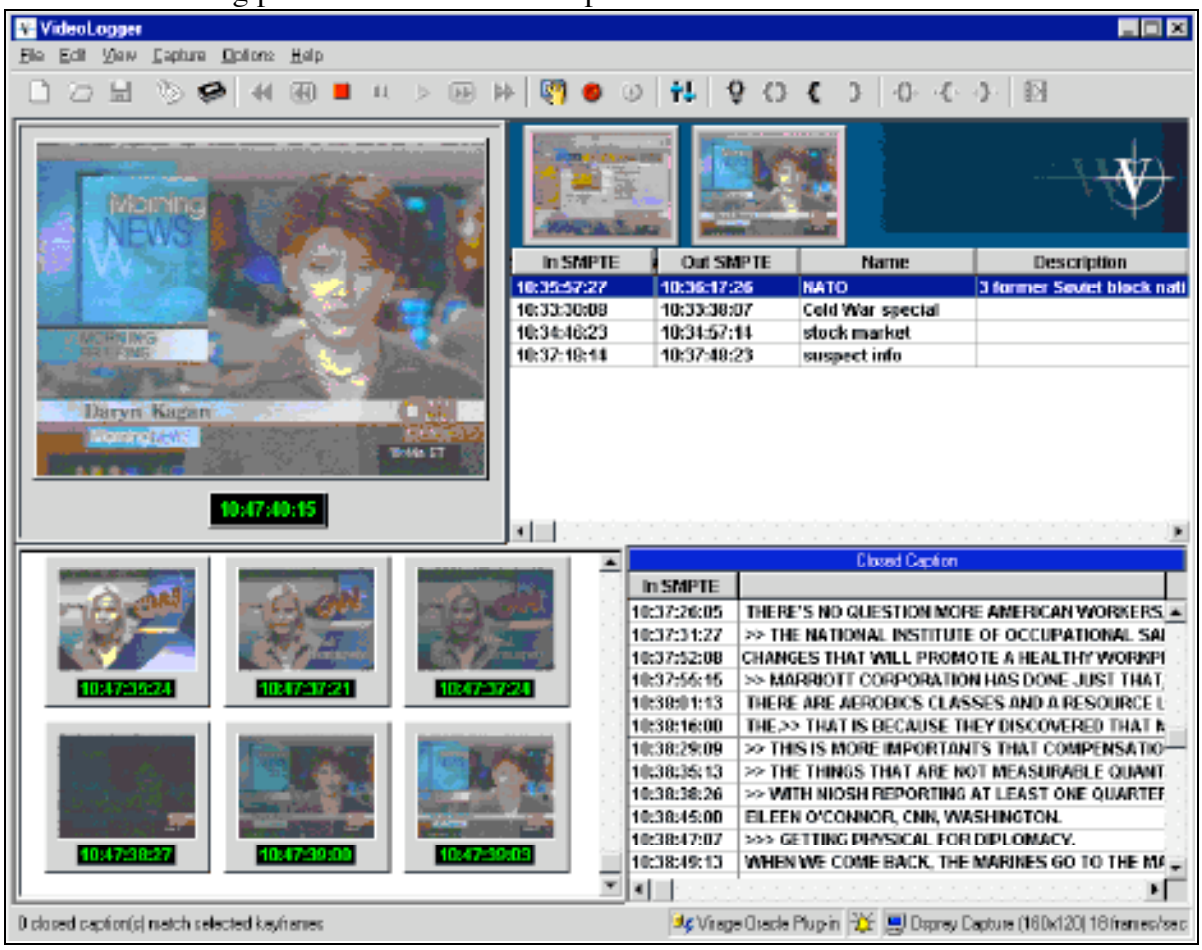

Figure 24: Video cataloger for harvesting open source television reports.

RESOURCE MATERIALS

Banchoff, Thomas, F., 1990. *Beyond the Third Dimension,* New York, New York: W.H. Freeman and Company.

Christensson, S.A. and A.E.R. Woodcock, 1996. Metaphorical Constructs for Command and Control and Battle Management. In: *Proceedings of the Second International Command and Control Research and Technology Symposium*. Held in Market Bosworth, England.

Christensson, S.A. and A.E.R. Woodcock, 1997. Metaphorical Constructs for Command and Control and Battle Management II. In: *Proceedings of the Third International Command and Control Research and Technology Symposium*. Held at the National Defense University, Fort McNair, Washington, D.C.

Dockery, J.T. and A.E.R. Woodcock, 1993. *The Military Landscape: Mathematical Models of Combat*. Abington, Cambridge: Woodhead Publishing Company, Ltd.

Grube, G.M.A. (tr.) 1974. *Plato's Republic*. Indianapolis: Hackett Publishing Co.

Kaku, Michio, 1994. *Hyperspace*, New York, New York: Doubleday.

Poston, T. and I.N. Stewart, 1978. *Catastrophe theory and its applications*. London: Pitman.

Richardson, S.B., A.E.R. Woodcock, and L. Cobb, 1994. Cellular automata models of combat. In: *Proceedings of the First Workshop in Command Information Systems*. Great Malvern, England: Defence Research Agency.

Rucker, Rudy, 1984. *The Fourth Dimension: A Guided Tour of the Higher Universes*, Boston: Houghton Mifflin Company.

Szyperski, Clemens, 1998. *Component Software: Beyond Object-Oriented Programming*, Addison-Wesley.

Sundin, C. and H. Friman, (eds.) 1998. *ROLF 2010 A Mobile Joint Command and Control Concept*. Stockholm, Sweden: The National Defence College.

Thom, R., 1975. *Structural stability and morphogenesis*. Reading, MA.: W.A. Benjamin.

Tilelli, John, H (Gen.), 1998, Ulci-Focus Lens '97: Putting JV2010 into Practice, *Joint Forces Quarterly*, Autumn / Winter,76-80.

United States Joint Staff, 1998. *United States Joint Publication 3-13: Information Operations*.

Wiederhold, C., Wegner P., and Ceri S., 1992.*Toward megaprogramming*, Communications of the ACM, 35(11), 89-99.

Wildgen, W., 1982. *Catastrophe theory semantics*. Amsterdam, The Netherlands, and Philadelphia, PA.: John Benjamins Publishing Company.

Woodcock. A.E.R., 1995. Metaphorical Mapping: Transformations between virtual and reality; In: Woodcock, A.E.R., B. Lönnbom, B. Gustavson, and S.A. Christensson (eds.) *Proceedings of the Second International Conference on Military Applications of Synthetic Environments and Virtual Reality (MASEVR'95)*, Stockholm, Sweden: The Defence Material Administration (FMV).

Woodcock, A.E.R., L. Cobb, and J.T. Dockery, 1989. Models of combat with embedded C^2. V: Cellular automata. *International C.I.S. Journal,* 3(3): 5-44.

Woodcock, A.E.R., L. Cobb, and P. Langendorf, 1993. *Catastrophe theory analysis of indications and warnings and command and control*. In: Dockery, J.T. and A.E.R. Woodcock, 1993.

Woodcock, A.E.R. and M. Davis, 1978. *Catastrophe theory*, New York, New York: E.P. Dutton.

Woodcock, A.E.R, and J.E. Heath, 1999. Q-Analysis Assessments of Inter-Ethnic Relationships. In: Woodcock, Alexander and David Davis (eds.). *The Cornwallis Group IV: Analysis of Civil-Military Interactions*. Cornwallis Park, Nova Scotia: The Pearson Peacekeeping Press.

Woodcock, A.E.R. and T. Poston, 1974. *A geometrical study of the elementary catastrophes*. New York, New York: Springer-Verlag.

Zeeman, E.C., 1978. *Catastrophe theory: Collected papers*. Reading, MA.: W.A. Benjamin.

1.

2. Also: Guest Professor, The National Defence College, Stockholm, Sweden; Visiting Professor, Royal Military College of Science (RMCS) Shrivenham, England, U.K., and Corresponding Faculty Member, The Center for Computational Statistics and Probability, George Mason University, Fairfax, Virginia, U.S.A.