

Makkay, Imre

INFORMATION OPERATIONS FROM THE AIR. STRATEGY AND TECHNOLOGY OF C2W

The competition for information is as old as human conflict. Nations, corporations, and individuals each seek to increase and protect their own store of information while trying to limit and penetrate the adversary's.

Information technology advances are making dramatic changes in how the nations fight wars in the nearest future. The intelligence-surveillance-reconnaissance capability will allow a commander's vision and view of the battlespace to be shared at the lowest level.

There is a main task the common understanding of how to use information warfare, information operations, command control warfare technology and tactics to enhance Air Force and joint warfighting capabilities.

FUNDAMENTALS OF INFORMATION OPERATIONS

Since 1970 th, there have been extraordinary improvements in the technical means of collecting, storing, analyzing, and transmitting information. Articles have been written about the impact of this technical revolution on the conduct of war, particularly since DESERT STORM.

What is information? Information derives from phenomena. Phenomena, observable facts or events, are everything that happens around us. Phenomena must be perceived and interpreted to become information. Information, then, is the result of two things: PERCEIVED PHENOMENA (data) and the INSTRUCTIONS required to interpret that data and give it meaning.

There is a familiar paradox: If a tree falls, but no one was around to hear it, did it make a noise?

The falling tree caused pressure waves in the atmosphere, a phenomenon. Noise, the information denoting a falling tree, occurs when someone's ear detects the pressure waves, creating data, and the brain's instructions manipulate that data into the sound recognizable as a falling tree. Within that person's context, there is no falling tree until the person hears (or sees) it.

Phenomena become information through observation and analysis. Therefore, information is an abstraction of phenomena. Information is the result of our

perceptions and interpretations, regardless of the means. As falling trees make clear, to define information requires only two characteristics: INFORMATION: DATA AND INSTRUCTIONS. INFORMATION FUNCTION: any activity involving the acquisition, transmission, storage, or transformation of information [6].

MILITARY INFORMATION are the counter to the *fog of war*. The commander with better information holds a powerful advantage over his adversary. Military operations make special demands on information functions in seeking to give the commander an information advantage.

Intelligence, surveillance, reconnaissance and weather analysis are the bases for orienting observations. Precision navigation enhances mission performance. Together, these are the kinds of military information functions that enhance all military operations.

MILITARY INFORMATION FUNCTION: any information function supporting and enhancing the employment of military forces.

Information warfare consists of targeting the enemy's information and information functions, while protecting our own, with the intent of degrading his will or capability to fight.

INFORMATION WARFARE: *any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.*

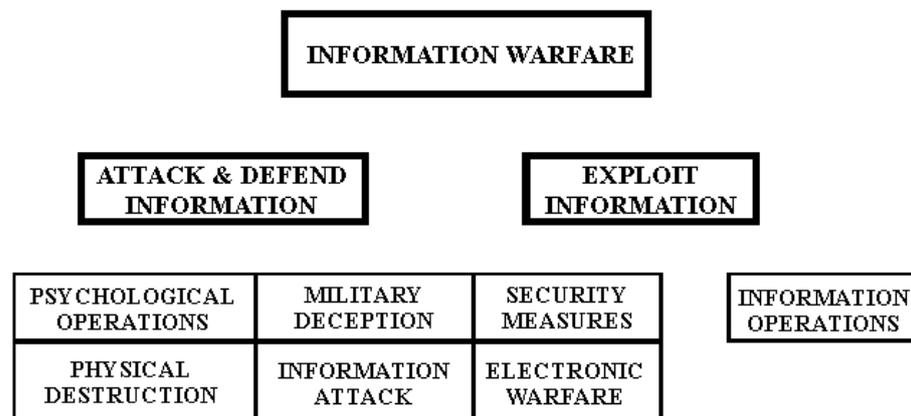


Figure 1. Information Warfare Structure

PSYCHOLOGICAL OPERATIONS use information to affect the enemy's reasoning.

ELECTRONIC WARFARE denies accurate information to the enemy.

MILITARY DECEPTION misleads the enemy about our capabilities or intentions.

PHYSICAL DESTRUCTION can do information warfare by affecting information system elements through the conversion of stored energy to

destructive power. The means of physical attack range from conventional bombs to electromagnetic pulse weapons.

SECURITY MEASURES seek to keep the adversary from learning about our military capabilities and intentions

INFORMATION ATTACK: directly corrupting information without visibly changing the physical entity within which it resides.[6]

INFORMATION OPERATIONS (IO): involve ACTIONS TAKEN TO AFFECT ADVERSARY INFORMATION AND INFORMATION SYSTEMS while defending one's own information and information systems. They apply across all phases of an operation, the range of military operations, and at every level of war. They are a critical factor in the joint force commander's (JFC's) capability to achieve and sustain the level of information superiority required for decisive joint operations. MANY DIFFERENT CAPABILITIES AND ACTIVITIES MUST BE INTEGRATED to achieve a coherent IO strategy¹.

OFFENSIVE INFORMATION OPERATIONS involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers and achieve or promote specific objectives. These assigned and supporting capabilities and activities include, but are not limited to, operations security (OPSEC), military deception, psychological operations, electronic warfare (EW), physical attack/destruction, and special information operations (SIO), and may include computer network attack.²

DEFENSIVE INFORMATION OPERATIONS integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive IO are conducted through information assurance, OPSEC, physical security, counterdeception, counter-propaganda, counterintelligence, EW, and SIO. Defensive IO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. Offensive IO also can support defensive IO.³

There are three objectives of information warfare:

- CONTROL the information realm so we can exploit it while protecting our own military information functions from enemy action,
- EXPLOIT control of information to employ information warfare against the enemy, and,
- ENHANCE overall force effectiveness by fully developing military information functions.

¹ JP 3-13

² JP 3-13

³ JP 3-13

THE RELATIONSHIP BETWEEN INFORMATION WARFARE AND COMMAND & CONTROL WARFARE

COMMAND AND CONTROL: *the exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission*⁴.

The focus of information warfare is *any* information function, whether it is C2, a refinery's control system, or a telephone switching station. Command and control warfare (C2W) only addresses activities directed against the adversary's ability to direct the disposition and employment of forces, or those which protect the friendly commander's ability to do so. Command and Control Warfare is only a particular application of information warfare.

Information Operations from the Air

Information superiority—the degree of dominance that allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition.

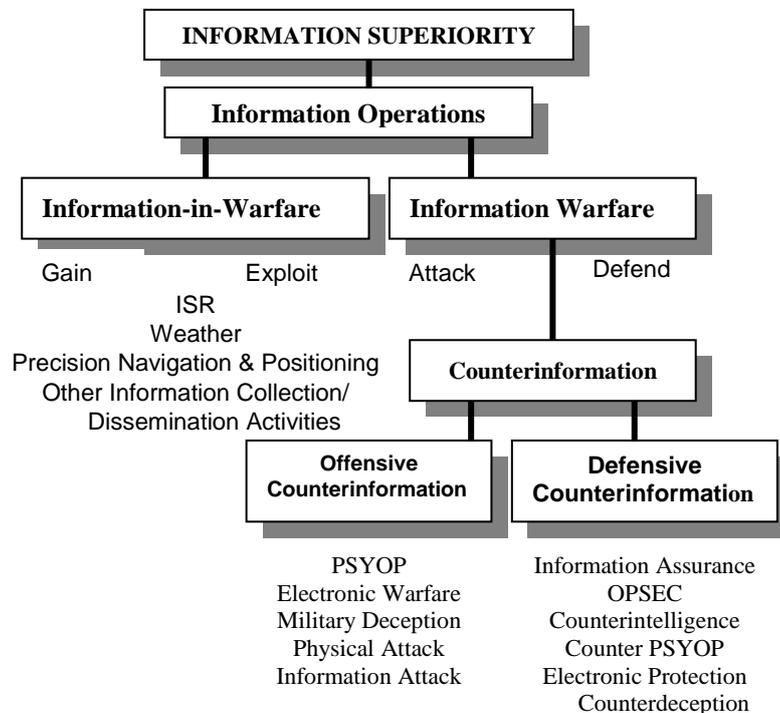


Figure 2. Information Superiority Construction

⁴ Joint Pub 1-02

PSYCHOLOGICAL OPERATIONS PSYOP are de-signed to convey selected information and indicators to foreign leaders and audiences to influence their emotions, motives, objective reasoning, and ultimately their behavior to favor friendly objectives. *PSYOP have strategic, operational, and tactical applications.* At the strategic level, PSYOP may take the form of political or diplomatic positions, announcements, or communiqués. At the operational and tactical levels, PSYOP planning may include the distribution of leaflets, the use of loudspeakers, and other means of transmitting information that encourage adversary forces to defect, desert, flee, or surrender and to promote fear or dissension in adversary ranks. Persistent PSYOP attacks can have a synergistic effect, accelerating the degradation of morale and further encouraging desertion.



Figure 2. COMMANDO SOLO aircraft for the psychological operations

Commando Solo is an airborne electronic broadcasting system utilizing four EC—130E RivetRider (RR) aircraft. Commando Solo conducts psychological operations and civil affairs broadcast missions in the standard AM, FM, HF, TV and military communications bands. Missions are flown at maximum altitudes possible to ensure optimum propagation patterns. This system may also be used to:

- Support disaster assistance efforts by broadcasting public information and instruction for evacuation operations;
- Provide temporary replacement for existing transmitters or expanding their areas of coverage;

- Other requirements, which involve radio and television broadcasting in its frequency, range.

Commando Solo capabilities can support civil actions by broadcasting via radio or TV:

- Educational programs and telecasts;
- Messages/speeches by government officials of friendly countries;
- Entertainment and cultural programs.

The EC—130 flies during either day or night scenarios and is air refuelable. A typical mission consists of a single-ship orbit, which is offset from the desired target audience. The targets may be either military or civilian personnel. Secondary missions include command and control communications countermeasures (C3CM) and limited intelligence gathering.

In the world of Electronic Combat, the major players are the EF—111 “Ravens”, F—16 “Fighting Falcons” and the EC—130H “Compass Call”. Forming the EC triad, these forces:

- Jam targets;
- Insert deception to confuse;
- Destroy critical targets.



Figure 3. EF—111 and F—16 patrolling in DESERT

COMPASS CALL is the designation for a modified version of the C—130 “HERCULES” aircraft configured to perform tactical command, control, and communications countermeasures. Specifically, the aircraft uses noise jamming to prevent communication or the transfer of information essential to command and control of weapon systems and other resources. It primarily supports tactical air operations but also can provide jamming support to ground force operations.

The RC—135V/W RIVET JOINT surveillance aircraft are equipped with an extensive array of sophisticated intelligence gathering equipment enabling military specialists to monitor the electronic activity of adversaries. Also known as “RJ”, the aircraft are sometimes called “hogs” due to the extended “hog nose” and “hog cheeks”. RIVET JOINT has been widely used in the 1990's — during Desert Storm, the occupation of Haiti, and most recently over Bosnia. Using automated and manual equipment, electronic and intelligence specialists can precisely locate, record and analyze much of what is being done in the electromagnetic spectrum.

The EA—6B PROWLER is the primary tactical jamming aircraft of the US Navy, US Air Force and the US Marine Corps. The Prowler first entered service in the 1970s and has demonstrated its battlefield performance in Southeast Asia, in Operation Desert Storm and in response to the crises in Bosnia- Herzegovina and in Kosovo. The aircraft operates from aircraft carriers and from forward land bases. The mission of the aircraft is to accompany the strike forces and to carry out armed reconnaissance, electronic warfare and jamming operations.



Figure 2.4. EA-6B *PROWLER* inside

The primary naval role is to protect the US or allied carrier group and aircraft by countering hostile radar and by jamming enemy communications. The Prowler also carries out electronic surveillance tasks and provides defense against incoming anti-ship missiles. The Prowler is armed with the Raytheon HARM High Speed Anti-Radiation Missile, AGM—88. The HARM missile is used against land-based and seaborne radar-directed air defense artillery systems and surface-to-air missile systems.

CONCLUSION

The Air Force, with its global perspective and experience, is uniquely qualified and positioned to play a leading role in developing and applying important new capabilities in the 21st century.

There are two aspects of information operations that help achieve information superiority: IIW, the traditional collection and exploitation, and IW, the “attack and defend” aspects. This document has focused primarily on IW, but IW must always be applied in operations that are fully coordinated with the IIW pillar and that are integrated into the wider aerospace operations plan.

IO FROM THE AIR — as a vital part of military operation in the information age - must be a valuable objective of science research work at National Defense University Doctor School also. Author recommend to join the Electronic Warfare Department science program at: <http://www.zmne.hu/tanszekek/ehc/research.htm>

LITERATURE

- [1] Information Operations Air Force Doctrine Document 2-5
- [2] “Joint Doctrine for Information Operations,” Joint Pub 3-13,
- [3] Electronic Warfare Air Force Doctrine Document 2-5.1
- [4] Psychological Operations Air Force Doctrine Document 2-5.5 22 February 1997
- [5] Special Operations Air Force Doctrine Document 2-7 September 1998
- [6] Ronald R. Fogleman, Sheila E. Widnall CORNERSTONES OF INFORMATION WARFARE <http://www.af.mil/lib/corner.html>
- [7] Dr. Várhegyi István, Dr. Makkay Imre Információs korszak, információs háború, biztonságkultúra OMIKK Budapest 2000