CHAPTER 4

INFORMATION EXPLOITATION

All the business of war, and indeed all the business of life, is to endeavour to find out what you don’t know from what you do; that’s what I called guessing what was at the other side of the hill.

The Duke of Wellington

Throughout history, success in conflict has depended on the ability of combatants to obtain information of military relevance on their opponents. This information can take many forms and may include: force dispositions, structures, organizations and capabilities. With rigorous analysis, information can be assessed to offer commanders an indication of an opponent’s potential intent. Military information is, therefore, a vital element of campaign planning. Information helps to determine potential lines of operation, decisive or critical points and centres of gravity at the military strategic and operational level, all related to the desired end-state or objective. Air power platforms and systems play a vital role in gathering data and information; thus, the timely exploitation of information is a key core capability of air power.

The aim of this chapter is to examine the decision/action cycle, to outline the methods used to gather, control and fuse information, to describe the types of systems involved, including the detailed considerations which apply to space operations, and to highlight the link to information operations and command and control warfare (C2W).

The Decision/Action Cycle

The fundamental output which all commanders seek from reconnaissance, surveillance and information systems is the timely provision of information to aid the commander’s decision making process. Information allows a commander to make decisions more quickly than his adversary. This process is known as the decision/action cycle, highlighted during the Korean War by Colonel John Boyd¹, a USAF pilot. Following his experience in air-to-air combat he devised the concept of observe, orientate, decide and act as a generic model for military decision making known as the ‘OODA’ loop. This is illustrated in Fig. 4.1.

¹ Boyd devised this model as a young Lieutenant in Korea. He served with distinction in the USAF, retiring as a Colonel. After his retirement he served, until his death in 1997, as a consultant to the USAF in the Pentagon. Much of Boyd’s thinking and teaching underpins Warden’s ‘Air Campaign’.
The core of Boyd’s model is to observe the enemy’s movement, orientate friendly forces to this movement, make a decision on what is to be done and act before the enemy acts. Within this construct, the result should be to force the enemy to become reactive to the initiative of friendly forces. In any joint, combined and multinational campaign, air power systems play a critical role in providing the information to allow the full potential of friendly systems to be brought to bear at the right time and place.

Information, Surveillance and Reconnaissance

Information
All air power platforms and systems are capable of gathering information. The information can take many forms ranging from the visual report of aircrews to the provision of sophisticated data from space-based remote sensors. Data can be gathered by many means including cameras, radars or electronic systems and assessed or processed to create militarily useful information. The assessment of information is a critical role for the commanders, aircrews and staffs engaged in information exploitation operations.

Surveillance
Surveillance is the systematic observation of aerospace, surface and sub-surface areas, places, persons or objects by visual, aural, photographic, electronic or other means.

Reconnaissance
Reconnaissance is the obtaining of information about the activities and resources of an opponent, or data concerning the meteorological, hydrographic or geographic characteristics of a particular area.
Targeting

The critical importance of the correct and timely targeting of air power is emphasised in Chapter 3 in terms of command and control and Chapter 6 in targeting for strategic effect. The provision of data and information on potential targets is a key role for air power in any campaign. Air power sensors and systems provide images and data on individual and groups of targets which may range from the national infrastructure of an opponent to individual units in fielded forces. Critical vulnerable nodes can be identified by contingency planning to allow commanders to be presented with a range of options.

Combat Assessment

Combat Assessment is another vital part of information exploitation and consists of three component parts: Battle Damage Assessment, Weapons Effects Analysis and Re-attack Recommendations. A general description of Battle Damage Assessment is below. Weapon Effects Analysis is carried out to ensure that an appropriate weapon was used to attack the target and that it functioned correctly. When the results of Battle Damage Assessment and Weapon Effects Analysis are combined, a Re-attack Recommendation can be made if necessary.
Battle Damage Assessment (BDA)

BDA is the recording of mission success by photographic or electronic means and is both an integral part of the targeting process - to avoid unnecessary re-tasking - and part of the employment of air power as a political tool in Peace Support Operations (PSO) or coercive operations. Photographs and videos showing Precision Guided Munitions striking targets without collateral damage, may be a critical part of the political campaign to retain or sustain public support and stay within the decision/action cycle of an opponent.\(^1\)

During the Gulf War, coalition forces encountered some difficulty in locating the militarily ineffective, but politically destabilizing, mobile SCUD missile systems. Increasing reliance had come to be placed on satellite sources, and a combination of insufficient numbers and bad weather, quite apart from the problems of speedy dissemination of intelligence to operational units, reduced their effectiveness in war. Consequently, the six Royal Air Force Tornado GRIAs were to make a contribution out of all proportion to their numbers. Tornado GRIAs were the first reconnaissance aircraft to be equipped with video recording of sensors operated by day and by night. In all, 140 missions were flown, without loss by the GRIAs, over enemy territory against a variety of targets, including SCUD mobile missile launchers. The versatility of the Tornado was a timely reminder of the value of a flexible, manned, intelligence gatherer when the limitations of unmanned systems, both tactical and strategic, had been exposed in a fast moving combat environment in an uncertain climate.

\(^1\) Full details are given in the RAF Air Operations manual.
Data Characteristics

Modern technology allows manned, unmanned and space-based reconnaissance systems to provide photographic, infra-red, radar and electronic data. In the context of air power doctrine, it is essential that commanders understand the strengths and weaknesses of the medium in which data has been gathered. For example, although aerial photography presents a two-dimensional picture, modern exploitation systems allow a great deal of precise measurement detail to be gained. Space-based sensors, however, may take time to switch from one area of interest to another and have a fixed interval between passes over an area of interest. For example, during the Gulf War British and French manned reconnaissance aircraft were employed to fill gaps in the satellite coverage to aid the process of combat assessment.

Databases

Another facet of information gathering is the establishment and maintenance of databases, which are a vital ingredient of the targeting process - itself a vital ingredient of the exploitation of air power's capability. The UK maintains an independent strategic database capability for both photographic and electronic data. This capability is covered in greater detail in the RAF Air Operations manual. The ability to share photographic and electronic data with potential allies remains a key element of coalition operations. Agreements and memoranda of understanding which prepare commanders and staff in advance to share the data gathered by air and space platforms are important factors to consider when carrying out contingency planning.

Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR)

When the collection and exploitation of intelligence is coordinated within the targeting process, the combined activity is known as ISTAR. In addition to the fusion of data, the fusion of commanders and staffs may be the critical organizational requirement to ensure that ISTAR resources are correctly employed. In multinational operations, the sharing of intelligence, information and data may require a flexibility of approach by both commanders and staffs to prevent barriers from being created. If ISTAR assets are not properly exploited and data is not fused in a timely manner, the knowledge edge for friendly forces may well be eroded.
Information Flow

- **Reporting.** The rapid dissemination of data gathered by air and space systems is an essential element of timely information exploitation. In-flight reports from aircrews, imagery gathered from aircraft and space systems and the initial assessment of those data, need to be passed to the appropriate level for the information to be exploited to best effect in support of the joint campaign. This requirement may require firm priorities to be set by commanders.

Orders. Information flow from headquarters can be complex. If coalition warfare is a predominant theme for future operations, the need for interoperability is essential. Contingency planning prior to deployment can help to develop procedures in order to create better understanding. Language barriers can be a particular problem in coalition operations. It is essential that orders are clearly understood by all force elements.
Internal Flow. It is essential that staff priorities do not impede the flow of information within deployed and operational air headquarters. As Chapter 3 makes clear, the JFACC exercises mission command on behalf of the JTFC. To do so effectively requires a timely flow of relevant information. Air planners at all levels - JFHQ, JFACC or CAOC - may find they spend a great deal of time in coalition, liaison and coordination to ensure that commanders are not swamped with large amounts of irrelevant military information.

Command and Control in the Gulf War

During the Gulf War, Coalition forces operated under both administrative and operational or war-fighting chains of command. All forces were brigaded under the overall command of the American General, Norman Schwarzkopf. Forces with specialized missions, such as the Czechoslovak chemical decontamination unit or the Polish field hospital, were incorporated into the administrative chain. Central Command was subdivided into 7 subordinate headquarters, broadly along functional lines. Joint Force Command, commanded by Prince Khalid Bin Sultan, a member of the Saudi Arabian Royalty, was the most complex of the various chains of command because it incorporated so many different national forces. A further complication was the partners’ differing national agendas that affected the operations of their military units. In one case, a Syrian Armour Division was given an operational reserve mission because the Syrian leadership would not commit to participating in an offensive to liberate Kuwait. The Pakistani contingent was even more restricted, and was tasked with guarding Islamic shrines.

Information Fusion

Data fusion is the assembly of information gathered from all sources into information which allows timely exploitation within the context of the campaign plan. Within a joint, combined or multinational headquarters, data and information will be available from a myriad of sources. A critical requirement for ISTAR commanders and staffs, therefore, is the timely fusion of information to commanders at the right time and place.

The task of information fusion may fall to either a deployed unit within the theatre of operations, or to higher headquarters. This is particularly true of the targeting process. This process can be complex and may require the fusion of information from a wide variety of national, military and non-military sources. In discrete operations such as PSO, political interest in the targeting of air power will always be high and it is likely that commanders and staffs will have to spend a great deal of time in liaison with national capitals.

---

3 AWC-sponsored Courses such as the Air Battle Staff Course (ABSC) and the JFACC Course emphasise this requirement.
4 See J H Nadel, “Command and Control” in Military Lessons of the Gulf War Part VI.
The fusion of data to aid the targeting process could be a key determinant in defining mission success. Therefore, the need for all involved in the provision of information to commanders to avoid swamping commanders provides another mission command challenge.

Air power platforms and systems which gather and provide information take many forms. In addition to large manned platforms such as AWACs and manned strategic and tactical reconnaissance aircraft, information can be gathered by unmanned aerial vehicles or space-based systems. The next section offers considerations for space operations.

Space Operations

The Space Environment

Space assets operate in an environment characterised by the laws of orbital motion, high energy particles and fluctuating magnetic fields and temperatures, while terrestrial air assets operate in the earth’s atmosphere.

Operational Implications

Space assets can have influence at all levels of warfare and over all types of conflict. The exploitation of information derived from space is ubiquitous in support of joint and multinational operations. The use of space began during the Cold War for military purposes. Increasingly, however, the rapid commercial development of space to allow greater information flows and data exchanges means that access to information gathered from space-based systems becomes easier and cheaper. As a result, in addition to the exploitation of space by friendly forces, it is likely that opponents will also exploit information gathered from space.

Fundamental Considerations

- **Positioning.** A satellite’s position is predictable because it is based on the mechanics of its orbit. The plane of its orbit must pass through the centre of the Earth, and its speed of circumnavigation is dictated by its altitude. Geo-stationary satellites are placed over the plane of the equator and at a single altitude which matches their speed with that of the Earth’s rotation.

- **Decisive Positions.** Geo-synchronous, semi-synchronous and sun-synchronous orbits are all key locations.

- **Global Coverage.** Global coverage is dependent on the altitude and type of orbit of the satellite or a constellation of satellites. Altitude and type of orbit are, however, relative terms and may define the role of a satellite. There is a finite interval between satellite passes over a particular location. There is, therefore, a period of time before a satellite can obtain and deliver the information required.
Manoeuvre. Suitably equipped satellites can change their orbit to deliver payload or to aim sensors or communications antennae. However, orbital manoeuvre is expensive in use of fuel, which can reduce a satellite’s operational life. Manoeuvre is normally reserved for high priority missions.

Cost/Access. Large capital investment in infrastructure, technology and training are required to deploy, maintain and sustain space-based assets. Within a coalition, nations may pay to use another nation’s space services or agree to share expenses. Countries may also access space by purchasing commercially available information.

Space Roles
There are four generic space roles:

Space Support
Space support missions are required to maintain and sustain military equipment and personnel in space. Missions include the launch of satellites, maintaining and sustaining equipment in orbit and the deployment of ground terminals.

Force Enhancement
Force enhancements improve the ability of space-based military forces to act as force multipliers by:

Surveillance and Reconnaissance. Space-based surveillance and reconnaissance systems offer global access, have a high collection volume and are highly responsive. They can provide near-real-time data across the electro-optical range. Radar surveillance can provide imagery day or night in any weather conditions at relatively low resolution. Optical reconnaissance satellites can produce high resolution imagery in a number of wavebands, but are subject to weather limitations. Surveillance satellites are an integral part of strategic warning systems whilst reconnaissance satellites can help to generate target details, imagery and mapping data, and perform combat assessment tasks.

Navigation. The Global Positioning System (GPS) is a US navigation system designed to provide US and Allied military forces with world-wide, 3 dimensional position, velocity and time information. GPS data aids air power platforms and systems in navigation, precision weapons delivery, photographic mapping, air-to-air refuelling and combat search and rescue operations. GPS is readily available to civilian and military users. Accuracy can be degraded by the service provider to those who do not have the appropriate level of decoding equipment and it is possible to jam GPS.
- **Communications.** Modern communications satellites carry multiple-beam steerable antennas to provide flexible coverage and to resist jamming. Communications capacity may, however, be limited by bandwidth and access port availability on satellites. Management of electro-magnetic spectrum capacity may be an important future function for component commanders.

- **Environmental Monitoring.** Space systems provide data on environmental factors which might affect air, land, maritime and special operations. Knowledge of these factors allows forces to avoid adverse environmental conditions while taking advantage of other conditions to enhance operations.

**Space Control**

Space control is analogous to control of the air. The function of space control operations is to gain and maintain space control as necessary in crisis or conflict to prevent the space forces of an opponent from influencing the outcome of terrestrial or space operations. Space control operations may be required to guarantee freedom of action for friendly forces. There are no systems deployed for space control operations (see below).

**Force Application**

Force application is the use of force from space against terrestrial (land, air and sea) targets in support of military operations. There are no systems deployed to provide force application (see below).

**Space Treaties and Interpretation**

The military use of space is constrained by national policy and international treaties. The primary treaty is the Outer Space Treaty of 1967, which has four major provisions: all countries have free access to space with liability for damage caused; space will be used for peaceful purposes; no weapons of mass destruction will be placed in orbit around the Earth or on the Moon; and all space objects must be registered with the United Nations. In addition, the outcome of the Strategic Arms Limitation Talks and subsequent bilateral agreements between the USA and USSR prevent the testing and deployment of space based anti-ballistic missile systems. This limitation remains in force, but may not apply multilaterally.

**Unmanned Aerial Vehicles (UAV)**

Manned reconnaissance assets available to a commander are generally limited in number, may be expensive to operate and require a highly trained crew. The UAV provides an additional capability enabling the theatre commander to conduct day or night reconnaissance, target acquisition and rapid BDA in near-real-time, within a high threat or heavily defended area, without risking the loss of a high value asset. A UAV can provide
target information and weapon designation at greater distances and less risk than the conventional system employing a Forward Air Controller.

UAVs will be used primarily by component commanders as a tactical reconnaissance, surveillance and target acquisition system. UAVs could be tasked in support of deception, special forces, maritime and combat search and rescue operations. They can also provide NBC, electronic warfare and weather reconnaissance. Tasking of UAVs should be integral to the established tasking procedures and not require separate provision. UAV operations will need to be integrated into airspace management and control systems to ensure safe separation between manned and unmanned aircraft and to notify friendly air defence systems.

Information Operations

The effective exploitation of information by air power platforms and systems may include the ability of air power systems to contribute to information operations. Information operations can take many forms and are covered by specialist doctrine in JWP 2-00 and equivalent NATO doctrine.

Information Operations enable the commander to make effective use of military capability and information within a framework of offensive and defensive measures. The overall policy for and conduct of Information Operations is a national issue and lies outside the scope of this document. In military terms, a commander may need to achieve information superiority by the use of Command and Control Warfare (C2W) and other information-related activities.

**Command and Control Warfare (C2W)**

The integrated use of all military capabilities including Physical Destruction, Electronic Warfare (EW), Deception, Information Support Operations and Operations Security supported by all-source intelligence and Communications and Information Systems (CIS), to deny information to, exploit, influence, degrade, confuse or destroy enemy C2 capabilities and to protect friendly C2, Intelligence and CIS against such actions.

Within the context of information exploitation, commanders may be required to mount information support operations which could include deception operations and operations to preserve command and control information system integrity and operational security. Air power platforms and systems have an important contributory role in information and information support operations.
Elements of C2W

The five C2W elements are Destruction, EW, Military Deception, Information Support Operations and Operations Security (OPSEC). Air power roles and missions are covered in greater detail in Chapter 7. A key feature of C2W is that the various elements can be integrated, which can offer disproportionate impact within a joint campaign. The five elements are described below.

Destruction

- **Offensive C2W.** Destruction operations are most effective when timed to occur just before an opponent needs a certain C2 function and may include attacks with standoff precision guided munitions, cruise missiles, conventional bombs, air-to-surface missiles or guns. The force mix will be determined by the nature of the campaign and the effect sought upon the target sets.

- **Defensive C2W.** Protection against destructive attack is provided by physical hardening, dispersal, redundancy and concealment techniques, which are applied individually or in combination to critical C2 assets.

Electronic Warfare (EW)

EW is military action taken to exploit the electromagnetic spectrum. It may have offensive and defensive components and is covered in more detail in Chapter 8.

Military Deception

Deception operations degrade the accuracy of hostile intelligence, surveillance, target acquisition and reconnaissance resources and seek to lead an adversary to draw the wrong conclusions from what he sees. The best deception reinforces perceptions in the enemy’s mind that can be exploited. Air power can make an important contribution to military deception operations.

Information Support Operations

Information Support Operations are planned to convey indicators to an opponent, favourable to our policy objectives, in an attempt to influence attitudes, emotions, motives, objective reasoning and ultimately their behaviour. Air power involvement in Information Support Operations could include: aircraft-based leaflet drops and facilities for the preparation of material, or airborne radio and TV transmission capabilities for the projection of Information Support Operation messages direct to foreign forces and civilian populations.
Operation Security (OPSEC)

OPSEC is a process used for denying the enemy information about friendly intentions, capabilities or limitations. This is accomplished by identifying which actions can be observed by an enemy collection system, determining which indicators could be interpreted or pieced together to derive friendly intent, and developing and employing selected measures that eliminate or reduce friendly vulnerabilities to such actions. OPSEC may be an essential element of a campaign plan since it can be used to conceal friendly preparations for crisis or war. It requires strong links between intelligence and OPSEC staffs to reduce vulnerabilities.

Defensive Information Operations

Defensive information operations focus upon the defence of information, information-based processes, information systems and computer-based networks. Attacks against systems may be either direct or indirect. A direct attack may be made on the military information infrastructure. Access to this infrastructure could be made via the information systems of third parties which have an electronic inter-connection with military systems. An indirect attack may be made on a service upon which a military activity depends including public utilities, contractors and commercially-provided systems. Attack techniques could include:

- **Unauthorised Access (‘Hacking’).** Unauthorised access to a system to compromise the confidentiality, integrity or availability of information.

- **Software Modification.** Malicious computer codes may be inserted into software which could have an immediate or delayed effect such as network viruses.

- **Hardware Modification.** Unauthorised modification to the hardware component structure etched onto a silicon chip is virtually undetectable and will cause deliberate malfunction under specific circumstances. This process is known as chipping.

A balanced and cost-effective mix of countermeasures is required to provide a credible defensive information operation capability. These measures must deter, protect, detect and react to any attack on critical information activities.

- **Deter.** A well-defended military installation with a well-organised, effective and determined guard force will have a deterrent effect on any person or organisation planning a physical attack.
● **Protect.** A reasonable degree of protection can be provided by using a combination of information, computer, communications and physical security. This may reduce exposure but absolute protection cannot be guaranteed.

● **Detect.** The detection process is the most important defensive INFO OPS measure. This includes malicious code detection, system auditing, hardware and software configuration management and providing the appropriate training for personnel.

● **Reaction.** Reaction consists of 4 steps: prevention of further damage to the system with immediate operational response; assessment of information lost, corrupted or compromised; amelioration of the damage already sustained by reconfiguration of systems or pathways; and restoration of the system service, possibly at a degraded level.

**Information Exploitation**

The ability of air power platforms and systems to gather data remains an important core capability for the successful conduct of any joint or multinational campaign. Furthermore, the ability to fuse data into that which is pertinent and germane to the commander will be a critical factor in the battle to retain the initiative and stay within an opponent’s decision/action cycle. As systems proliferate, there is a risk that future commanders will be deluged with data and information. Therefore, successful information exploitation requires a holistic approach to the tasking and targeting of air power and the understanding and integration of space-based or UAV ISTAR assets. Nor can information exploitation be separated from the wider discipline of information operations - the timely exploitation of information may define the difference between success and failure in all military operations.