

INFORMATION OPERATIONS: THE IMPACTS ON C4I SYSTEMS

By

Albert R. Zehetner, Manager, Information Security Group
Electronic Warfare Associates – Australia
www.ewa-australia.com infosec@ewa-australia.com

Summary

This paper describes the vital and powerful relationship between Command, Control, Communications, Computers and Intelligence (C4I) systems and Information Operations (IO). The primary influence that IO provides the user of a C4I systems is a coordinated and integrated information picture to be accessed through the C4I system to aid decision-making, while at the same time complicating the information and information systems of an adversary. This relationship provides significant leverage towards obtaining information superiority and, ultimately, decision superiority.

However, the increasing use of information technology and IO also makes the C4I system more attractive to attack; hence, there is a need to secure C4I systems. This requires the use of security engineering and information security principles to be considered, which provide the user with an assurance that the system he or she is using to assist in making critical decisions is trusted and not compromised. In doing so information superiority is retained by friendly forces.

"The history of command can thus be understood in terms of a race between the demand for information and the ability of command systems to meet it."¹

Command and Control

The ability for a military commander to exercise command and control in the battlespace has improved with the advent of new technologies and practices. Command is defined as the authority vested in an individual for the direction, coordination and control of forces. Control is the analysis of requirements, resourcing, direction, coordination and monitoring of the effort. Command and control (C2) are intimately linked and rely upon communication and intelligence to facilitate decisions², and now increasingly upon the systems that support C2. The battlespace is becoming more complex, dealing with information from many different environments (land, sea, air, space, sensors, networks and data stores)³, which must be presented to the commander in a useful, timely and uncompromised manner to aid in decision-making.

C4I Systems

The commander seeks to utilise all resources available to him/her. Many of these resources have been available in 'traditional' warfare, however, a

number of new technologies have emerged. Merging the old and the new; personnel, procedures, C2, weaponry, communication and information systems can form a powerful augmented system used by the commander to conduct operations. One such system is the C4I system, which captures the essence of C2 in the current Information Age. C4I systems consist of people, procedures, technology, doctrine and authority and play an ever-increasing role in information management, data fusion, and dissemination⁴.

The purpose of a C4I system is to help the commander achieve his objective and the ultimate situation is where the commander achieves decision superiority over the adversary – in the classic Observation-Oriented-Decision-Action (OODA) cycle – so as to impose his/her intent (to accomplish the objective) upon the battlespace before the enemy can impose theirs. Decision superiority stems from information superiority, which can be described as the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same⁵. The crux of this situation is determining the value of the information gathered by own forces and preventing hostile forces obtaining or degrading own force information capabilities and data. Given this setting a capability termed "Information Operations" is employed to achieve information superiority for the commander.

Information Operations

The objective of IO is to augment military effort by promoting and protecting own force information and information systems while exploiting or degrading an adversary's information and information systems – a state of information superiority.

This paper considers the scope of IO to encompass military (Information Warfare) and non-military actions (Information Assurance) and is conducted during times of conflict and during peacetime. Further, there are many definitions in the available literature of what constitutes an Information Operations (IO) capability. This paper derives IO capability from the new draft USDOD Directive 3600.1⁶ and illustrated in Figure 1 below.

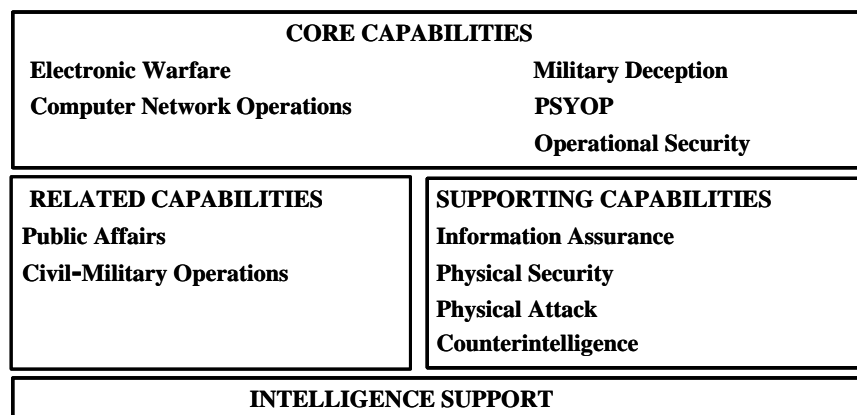


Figure 1: Information Operations Structure

It should be noted that the core IO capabilities are both offensive and defensive in nature and target people, information systems and physical infrastructure.

Information Offence and Defence

*"Information operations integrate all aspects of information to support and enhance the elements of combat power, with the goal of dominating the battlespace at the right time, at the right place, and with the right weapons or resources."*⁷

IO plays a significant part in providing a solution to a changing battlespace – it unites knowledge with the ability to respond. However, a cultural obstacle may exist in the employment of IO. Before the rise of IO as an integrated capability, many of these core capabilities in Figure 1 existed as mature and dedicated professional military streams in their own right. One of the challenges of the commander employing IO is to remove possible traditional barriers and integrate these capabilities into an effective, cohesive and successful force.

Electronic Warfare (offensive/defensive)

Electronic Warfare (EW) deals with utilising the electromagnetic spectrum for use by own forces while disallowing the same use by the adversary. The mechanics of EW can be simplified in terms of being a suite of sensors and effectors, both offensive and defensive in focus, to obtain information and use it to improve platform survivability, destroy enemy EW points of presence, etc. Such sensors could be linked to the commanders C4I system to provide vital data to many levels of command. In the network centric view of the battlespace, each EW sensor on an aircraft, ship, ground vehicle or soldier provides an input into the 'eyes and ears' of the C4I system and the anti-radiation missile or jammer pod could well be seen as an output (or the 'fist') from the C4I system – imposing the commander's will in the physical world. It should also be noted that enemy offensive EW tactics could destroy or incapacitate the same eyes, ears and fist of the commander that have become so valuable in the battlespace.

Computer Network Operations (offensive/defensive)

Computer Network Operations (CNO) consists of two specific yet complementary mission areas: Computer Network Defence (CND) and Computer Network Attack (CNA). The CND mission is to defend friendly computer networks and systems from any unauthorized event whether it be a probe, scan, virus, or intrusion. The CNA mission is to coordinate, support and conduct computer network attack operations in an effort to investigate, breach or otherwise compromise the enemy information systems⁸. Since the commander's C4I system is an information system comprising of computer elements, CND is vital to protect the integrity of the system and the information that flows within it. Further, feedback from CNA missions may assist the commander in determining the status and characteristics of the adversary's information systems. This information/information systems security aspect of C4I systems will be discussed later in this paper.

Military Deception (offensive)

Military deception is defined as being those actions executed to deliberately mislead adversary military decision-makers with respect to friendly military capabilities, intentions, and operations, and so causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission⁹. Military deception is an offensive capability utilised by the commander and with respect to the commander's C4I system, deception is more of an output (deciding to employ deception) or an input (receiving the results of deception operations to assist in further decision making) rather than an integrated part of the system.

Psychological Operations (offensive)

Psychological operations (PSYOP) induce or reinforce foreign attitudes and behaviours favourable to the originator's objectives by conducting planned operations to convey selected information to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, the behaviour of foreign governments, organisations, groups and individuals¹⁰. However, it is worth mentioning that adversarial PSYOP could pose a danger by compromising organic sensors (own force personnel) and thus degrading the integrity of the information fed to/actions required from the C4I system.

Operational Security (defensive)

"[Operational Security] OPSEC is a process used to deny to potential adversaries information about capabilities and/or intentions by identifying, controlling and protecting evidence of the planning and executing of sensitive activities. This process is equally applicable to government, its contractors, and to private enterprise in the protection of their trade secrets and other proprietary information. While military strength and capability still are required during the next years of uncertainty, we must likewise protect our critical economic information and technologies from those who seek to exploit them to their benefit and to our disadvantage"¹¹. OPSEC is a defensive measure employed to secure the C4I system from physical, information, personnel and related security threats. An OPSEC breach could reveal tactics and plans to an adversary and thereby compromise the value of the information for a mission.

Supporting Capabilities

The above core capabilities are incomplete without the supporting capabilities of information assurance (IA), physical security, physical attack and counterintelligence (CI):

- IA provides information security by ensuring confidentiality, authentication, integrity, non-repudiation, access control and availability¹² at all levels and locations for the military activity. Information security strives to achieve IA;
- Physical security may be considered a sub-element of OPSEC, although it applies to many other aspects such as C2 facility design, C4I system design, etc.;

- Physical attack remains a very effective means of disabling or destroying an adversary's capability and can come in many forms such as the anti-radiation missile strike on the SAM site, a precision guided munition delivered using geo-positional navigation systems, or a more 'traditional' means of achieving the objective; and
- CI strives to ensure that enemy intelligence threats such as human intelligence (HUMINT) are detected and neutralised as well as ensuring the relevance of PSYOP and public/civil affairs.

The entire IO gamut is backed by intelligence support provided by HUMINT, electronic intelligence (ELINT), imagery intelligence (IMINT), etc. that is all connected to the commander by information systems (including the C4I system) in real time and near-real time at various hierarchical levels and at many theatres of operation.

It is important to note that IO should entail all aspects of information, examined from both own force and adversary perspectives, and conducted from both offensive and defensive postures. Focusing merely on one aspect of the information (e.g., force deployment statistics or mission status) will invariably result in a failure to recognise a needed shift in perception or focus (e.g., logistics issues, CI updates, CND breaches, etc.) to keep ahead of the adversary. To successfully utilise IO as an integral part of military campaigns across the spectrum of conflict, the commander must develop a clear understanding of what information is useful to the military endeavour, and how it can be captured, managed, and exploited. This issue concerns the value of information in the C4I system to aid in obtaining information and decision superiority.

Information Superiority for C4I systems

"Full Spectrum Dominance... space, sea, land, air, and information"¹³

The vision of "Full Spectrum Dominance" may be realised using an effective IO capability that delivers a validated, correct and timely (assured) service to the commander. Information superiority is derived from a superior information position (a function of the attributes shown in Figure 2) and (hopefully) enables decision superiority which is the goal of the commander's support system. The commander can achieve domination of the battlespace by creating and maintaining a superior information position, i.e., having a larger volume (illustrated) than adversary.

IO capabilities enable a superior information position by providing information that is relevant to the geo-location, enemy forces, political situation, etc. from the many sensors and intelligence inputs to the C4I system. The end game is to "compress the kill chain", i.e., the six stage target cycle of "Find, Fix, Track, Target, Engage and Assess" or "F2T2EA"¹⁴. Adequate information supplied in real time and near-real time allows the commander to assess the situation (from the perspective of the area of operations (AO) combining wide area and local situational awareness), determine courses of action (force composition, available resources, targeting options, etc.) and execute a command (such as providing targeting information directly to the most effective weapon system in the

AO) that secures the objective. This is equivalent to shortening the OODA cycle.

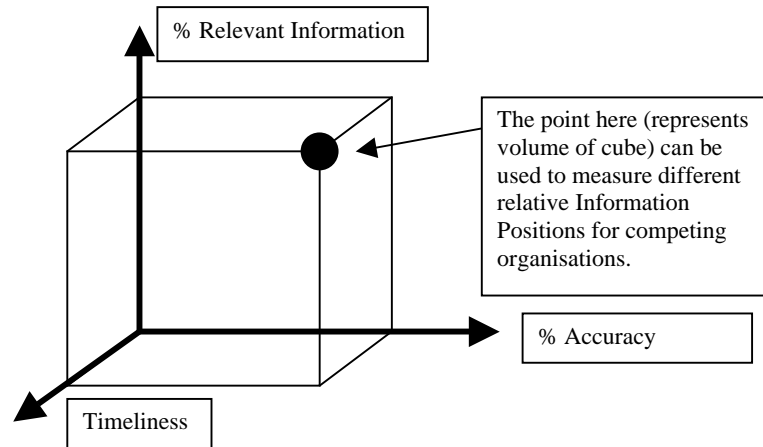


Figure 2: The Information Position¹⁵

A favourable scenario sees information required by the commander in a mature IO-enabled force already collected and available to the him/her in a user-friendly form through the C4I system. The inherent capabilities of IO also ensure integrity of data and systems and that the superior information position is maintained by the commander. It is important to note that the converse is true; without the C4I system, the IO effort may in fact be poorly coordinated and some actions may be nugatory or wasteful.

Security Considerations for C4I Systems

The IA attributes required by the commander of the C4I system have been discussed and, regardless of IO capabilities that seek to protect the system (OPESEC, CND, etc.), any networked information system that warrants protection will have a need for security considerations in all phases of its existence. Ultimately, the issues of data/system integrity and a commander's confidence will determine the value of a C4I system. Commanders and soldiers conducting information-enabled operations may not trust the information (and risk their lives) provided to them if it does not come with appropriate authority, is unprotected, tardy and unaccountable. Commanders desire an assurance that the data fed into their C4I systems is valid and trusted but also that such processes (being management-oriented) do not hinder the decision-making and order-disseminating process. It is the author's opinion that network security techniques employed in military, commercial and government arenas (and as noted akin to CND) will be required to reduce the risk to information security and increase IA.

The tenets of information security; confidentiality, integrity and availability should be considered; these will advance IA. The following examples briefly illustrate the importance of these tenets on the C4I system¹⁶:

- Plans and tactics must remain confidential for high mission success probability. Nondisclosure of critical information is supported by

effective OPSEC and the manipulation of the adversary through deception and PSYOP techniques;

- Information in the C4I system and supporting information systems (such as logistics information systems and medical records) must be accurate, for example, altered ammunition requests could lead to unplanned exhausted supplies too early in a mission; and
- The commander must be able to access the C4I system, communications links to superiors/subordinates/allies, etc. when required.

Security Engineering

A C4I system is like any other distributed information system, although the information that flows through it may have caveats imposed upon it and, as such, the tenets of information security should be 'engineered' into the solution together with other performance requirements. This section seeks to mention the unglamorous issues of design considerations, standards and best practice that should be considered in the design, operation and maintenance of a C4I system. Without these, own force IO is suboptimal, system use may be flawed (poor availability, non-robust design and subject to operator errors, etc.) and especially in the case of CND, the probability of an adversary compromising the system would significantly increase.

C4I system design from a security perspective involves a number of considerations that have found mature application in distributed system development¹⁷. There are a number of key considerations as follows:

- Security policy,
- System hardening/System security configuration management,
- Systems administration and management (access control),
- Monitoring and logging systems (audits, intrusion detection systems (IDS), etc.);
- Firewall deployment,
- Social engineering attack countermeasures (protocols and procedures),
- Use of encryption mechanisms,
- Multilevel security,
- Use of Biometrics,
- Physical security considerations,
- Emission security,
- Military CND tools and techniques, and
- User and support staff education.

All of these considerations represent best practice in the security engineering of modern systems, they are reiterated here to ensure their inclusion in the design development process along side the specifications for bandwidth, tactical interfaces, deployable characteristics, spares, etc. for the C4I system.

However, some of these 'hard' design characteristics need to be merged with 'soft' issues such as identifying and resourcing the security posture of the organisation and system, determining the risk exposure of a system to threats, and verifying these. Standards such as:

- ISO/IEC 17799 – *Information Technology – Code of Practice for Information Security Management* allows for a comprehensive security assessment;
- Australian Standard 4360 *Risk Management* and AS/NZS Handbook 231 – *Information Risk Management* provide an excellent basis for a threat and risk assessment of system and application development; and
- Common Methodology for Information Technology Security Evaluation CCIMB-2002-07-001 Supplement: *Vulnerability Analysis and Penetration Testing* provides a means of verifying the security of the system through vulnerability assessments and penetration testing.

These standard practices give the users and support personnel of the system a form of IA that is essential for a critical tool such as a C4I system.

Another means of obtaining assurance of information and systems is to certify the C4I system in accordance with a recognised standard. This is a foundation management technique that seeks to measure the capability in order to effectively plan and operate it. In relation to security engineering, initiatives by leading organisations such as the Information Assurance Technical Framework Forum (IATFF) and their publication IATF Release 3.1 (September 2002)¹⁸, and the International Systems Security Engineering Association (ISSEA)¹⁹ through their Security Systems Engineering – Capability Maturity Model (SSE-CMM), ISO/IEC 21827²⁰, provide a formal recognised method of establishing a framework for measuring and improving performance of security engineering solutions.

In combination, the above tools provide a sound basis for security design of systems that will assist the C4I system user and support staff achieve the IA requirements they desire.

Threat Detection and Response

Once a system is constructed and assessed the work does not end there. The system's threat and risk profile should be reviewed and active measures be put in place to provide system support staff with metrics and tools for information protection.

While preventing intrusion is the best case scenario, there are times when unauthorised access to the system occurs; it is then that the system support staff must know when the intrusion occurs, its nature and what the consequences of the intrusion are²¹. Intrusion detection techniques require careful consideration of policies, procedures, tools for detection and response²². The consequences of the intrusion will also depend upon the system architecture and the interfaces with other systems/applications. This is two-way, a compromise to the C4I system could lead to an attack on a medical records database, and conversely, an ammunition database may led the attacker to the wealth of information residing on the C4I system. An

IDS seeks to alert the system managers to prevent a host of attacks including, but not limited to²³:

- Unauthorised access to data (threat to confidentiality),
- Data manipulation (threat to integrity),
- Denial of Service (DOS) attack (threat to availability), and
- Establishing a 'beachhead' and using that as a staging area/launch point for further attacks²⁴.

System support personnel must then be able to respond to such attacks and return the C4I system to normal operations in order for the user to regain access to a trusted, valued tool. Improvement programs should also be institutionalised for organisations to learn from and prevent like attacks from reoccurring.

With so many possibilities of attacks by malicious entities, a holistic approach to network security should not be treated lightly. Without the incorporation of information security design considerations the C4I system will not be able to provide the commander with adequate assurances as to its value in the decision-making process, severely decreasing the information superiority afforded by IO. The optimal solution requires all three design areas to coexist in harmony.

Conclusion

It is the author's opinion that IO has a significant impact upon the operation and effectiveness of C4I systems. As it has been shown throughout this paper, IO provides an integrated, comprehensive, relevant, secured, and verified (from numerous intelligence sources) information service to the C4I system which is able to present said information in a usable manner to the user. This allows the user to achieve a superior information position over his or her adversary. It is not contested that a C4I system could function without an IO link, however, the performance of such a system would be less than one linked to IO capabilities. Conversely, IO relies upon a coordinated C2 approach (through a C4I networked information system) to allow for optimised operations.

However, the benefits provided by IO and, indeed, the C4I system itself, are not realised if the system not only achieves technical integrity (performs to specification) but also information security. Adversarial attacks on own systems can be met and responded through CND and security engineering practices. Once this is accomplished, the commander is placed in a sound position to attain decision superiority (the shorter OODA cycle) and also full spectrum dominance in the battlespace.

Author's Biography:

Albert Zehetner *MSc ME BE* manages EWA-Australia's Information Security Group and has been involved in EW and C2 military systems engineering projects, network and application information security activities. Prior to joining EWA, Albert was employed in the Australian Defence Organisation in a number of roles including engineering manager of a major capital acquisition project, airworthiness regulator, and tactical fighter ILSM at RAAF Williamstown.

References

- 1 Van Creveld, M. (1985), *Command in War*, Harvard University Press, Cambridge
- 2 Frater, M. and Ryan, M. (2001), *Electronic Warfare for the Digitised Battlefield*, Artech House, Norwood.
- 3 United States Department of Defense (USDoD) (1998), *Joint Publication 3-13*, "Joint Doctrine for Information Operations", 9 October 1998, Joint Chiefs of Staff, Washington, DC.
- 4 United States Department of Defence (USDoD) (1995), *Joint Doctrine for Command, Control, Communications and Computer (C4) Systems Support for Joint Operations*, Joint Chiefs of Staff, 30 May 1995, Available at http://www.dtic.mil/doctrine/jel/new_pubs/jp6_0.pdf
- 5 Ibid (Ref 2)
- 6 Deckro, R. and Hathaway, M. (2002), Information Operations Workshop Summary, *PHALANX*, Vol 35, Number 3, September 2002. Available: <http://www.mors.org/publications/phalanx/sep02/lead.htm>
- 7 Ibid (Ref 2)
- 8 Joint Task Force – Computer Network Operations (JTF-CNO), US Strategic Command (2002), "Computer Network Operations", Previously available from: <http://www.stratcom.mil/factsheetshtml/jtf-cno.htm>
- 9 Ibid (Ref 2)
- 10 United States Department of Defense (USDOD), (2000), US Special Operations Forces, *Posture Statement 2000*, "Providing Unique Solutions for a Changing World", Available: <http://www.defenselink.mil/pubs/sof/>
- 11 Operational Security (OPSEC) Professionals Society (2002), "OPS 2002", Available: <http://www.opsec.org/Overview.html>
- 12 Stallings, W. (1999), *Cryptography and Computer Security – Principles and Practice*, Second Edition, Prentice Hall, New Jersey
- 13 United States Department of Defence (USDoD) (2000), "Joint Vision 2020", Joint Chiefs of Staff Available: <http://www.dtic.mil/jcs>
- 14 Herbert, A. J. (2003), "Compressing the Kill Chain", *Journal of the Air Force Association*, March 2003, Vol. 86, No. 3
- 15 Alberts, D. S., et al (2000), *Network Centric Warfare: Developing and Leveraging Information Superiority*, Second Edition (Revised), CCRP Publication Series, Sun Microsystems Federal Inc.
- 16 Conversations with Alastair Sharman, EWA Queensland Operations Manager, Security and Intelligence Specialist
- 17 Anderson, R. (2001), *Security Engineering – A guide to building dependable distributed systems*, Wiley Computer Publishing, New York
- 18 www.nsa.gov and www.iatf.net
- 19 www.issea.org
- 20 www.sse-cmm.org
- 21 Allen, J. H. (2001), *The CERT guide to system and network security practices*, SEI Series in Software Engineering, Addison-Wesley, New Jersey
- 22 Defence Signals Directorate, Australian Communications–Electronic Security Instruction 33 (ACSI 33)
- 23 Proctor, P. (2001), *The Practical Intrusion Detection Handbook*, Prentice Hall PTR, New Jersey
- 24 Attributed to Ron Brandis, CISSP, EWA Senior Information Security Consultant