2006

An Information Operation Model and Classification Scheme

D T. Shaw
Edith Cowan University

S Cikara
Edith Cowan University

DOI: 10.4225/75/57a815b8aa0d1
Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.

An Information Operation Model and Classification Scheme

DT Shaw and S Cikara
School of Computer and Information Science
Edith Cowan University
Bradford Street
Mount Lawley
dtshaw@student.ecu.edu.au

Abstract

Information systems are used in overt and covert conflict and information operations target an opponent's ability to manage information in support of operations for political, commercial and military advantage. System level attacks are complicated by logistic problems that require resources, command and control. Node level attacks are practical but of limited value. Collocated equipment comprises a temporary node that may be feasibly attacked. Estimation of IW operation merits may founder on the difficulty of predicting the net benefit for the costs. Starting from with Shannon's model, a simple cost-benefit model is discussed. Existing models are extended by an IW attack classification. A notional attack on system hardware is discussed with some defensive measures.

Keywords

Records management, Information Warfare, hardware attacks, unauthorised modification

INTRODUCTION

Industrialised warfare, characterised as 'absolute war' in 1832 by Clausewitz, is material and labour intensive. The creation of armed services comprising millions of combatants and auxiliaries required organisation of labour and materiel with corresponding levels of management. With conflicting requirements and limited resources, efficient allocation is important. For example, operations research (OR) is '*the science of planning and executing an operation to make the most economical use of the resources available.*' (Macksey and Woodhouse, 1991, p. 18) Taha notes the importance of human (people) aspects (Taha, 1992, p. 2). It is noted that efficient resource usage may depend on a wide range of criteria including information and people. Logistic management relies on information management that currently relies on electronic information technology.

Modern 'Information Warfare' (IW) targets the information assets and infrastructure of an opponent in overt and covert operations. (Waller, 1995) Waltz describes three essential information infrastructure security properties as '*availability, integrity and confidentiality*' with respective IW objectives as '*disruption or denial, corruption and exploitation*'. (Waltz, 1998, pp.22-23)

However, IW operations require realistic assessments where military necessity is modified by external influences made powerful by information systems. In spite of IW opportunities, the existing constraints of armed conflict seem to be applicable in that '*Information Warfare weapons must meet the same tests for necessity and proportionality as other weapons under the laws of armed conflict.*' (Kuschner, 1998; Yurcik, 1997)

Ignatieff, discussing '*Virtual War*' or war with precision weapons and strong media component, suggests '*By 1999, military lawyers had been integrated into every phase of the air campaign, including the finalisation of the air tasking orders which assigned pilots to specific targets and missions.*' (Ignatieff, 2000, p. 197) He continues, '*But legal imperatives combined with public expectation are driving warfare towards 100 percent precision weapon use.*' (Ignatieff, 2000, p. 198)

It is noted that substantial information systems are needed for such operations and are also the target of such operations.

INFORMATION SYSTEMS

The Shannon Model (Slepian, 1974, pp. 5-29) describes fundamental characteristics of a communication system. The Transmitter sends the message in the channel to the Receiver. The channel is subject to inherent 'noise' that can be from natural and human sources. This model describes information flow between nodes and underpins associated analytic techniques.

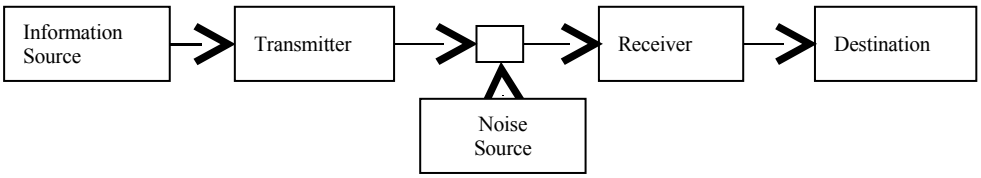

Figure 1 Shannon Model of an Information System

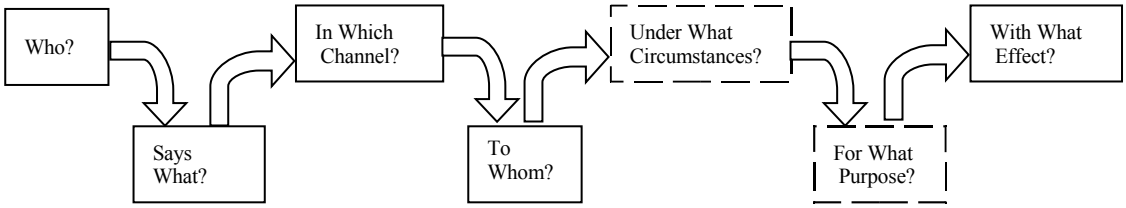

Figure 2 Lasswell – Braddock Model

Other models restate the basic Shannon relationship in various ways. Lasswell, speaking of Mass Communication, in 1948 stated '*A convenient way to describe an act of communication is to answer the following questions: Who? Says What? In Which Channel? To Whom? With What Effect?'*. This was extended by Braddock who interposes "*Under What Circumstances? For What purpose?*". (McQuail and Windahl, 1981, pp.10-11) The De Fleur model includes both transmission and reception 'Shannon' channels, addresses feedback and shows that noise is applied to all system components. (McQuail and Windahl, 1981, p.13)

Shannon	Lasswell - Braddock
-	For what purpose? Under what circumstances?
Sender	Who?
Message	Says what?
Channel	In which channel?
Noise	-
Receiver	To whom?
-	With what effect?

Figure 3 Comparison of Shannon and Lasswell-Braddock Models

Lasswell-Braddock can be recast as a 'Shannon Model'; however, it also addresses the intent and effect of the communication.

Shannon models may be concatenated to describe more complex systems or decomposed to show increasing detail. System characteristics include the probabilities of the correct message being received and bandwidth (Bytes per second) may measure information transfer between Sender and Receiver. It is noted that Transfer

Functions for each channel and node may become very complex in real world systems. However, the interface between node and channel is suitable for observing, measuring or interfering with messages.

CLASSIFYING ATTACKS ON INFORMATION SYSTEMS

Information security is primarily concerned on how to prevent or detect misconduct in information-based systems though information may have no physical existence. According to Stallings (Stallings, 1998), "*a computer system or network are best categorised by viewing the function of the computer system as providing information. In general, there is a flow of information from one source… to a destination*". Additionally, the model may be applied to any system where there is an exchange of information (Figure 4) and it complies with the Waltz objectives.

While this model depicts information exchange and possible attack scenarios there is a high level of abstraction. Interruption (Figure 4b) attacks availability when a system asset is destroyed, unavailable or unusable. Interception (Figure 4c) attacks confidentiality when an unauthorised party gains access to an asset. Modification (Figure 4d) attacks integrity when unauthorised parties gain access and also tamper with an asset. Fabrication (Figure 4e) attacks authenticity when unauthorised party successfully inserts counterfeit objects into the system.

Fisch and White bridge these gaps with '*Assessment Theory*' where '*the goals of a risk assessment are to identify the areas of a computer or network that are most susceptible to compromise and to determine the most appropriate protection for these areas'*. (Fisch and White, 2000) A threat measurement is presented with three binary classes (8 categories): Hostility, Sophistication and Source.

While it is less abstract than Stallings and offers greater detail by including the attacker intention (hostile versus non-hostile), the complexity (sophisticated versus unsophisticated) and threat source (internal or external), it does not explicitly address what, who, and by what means.

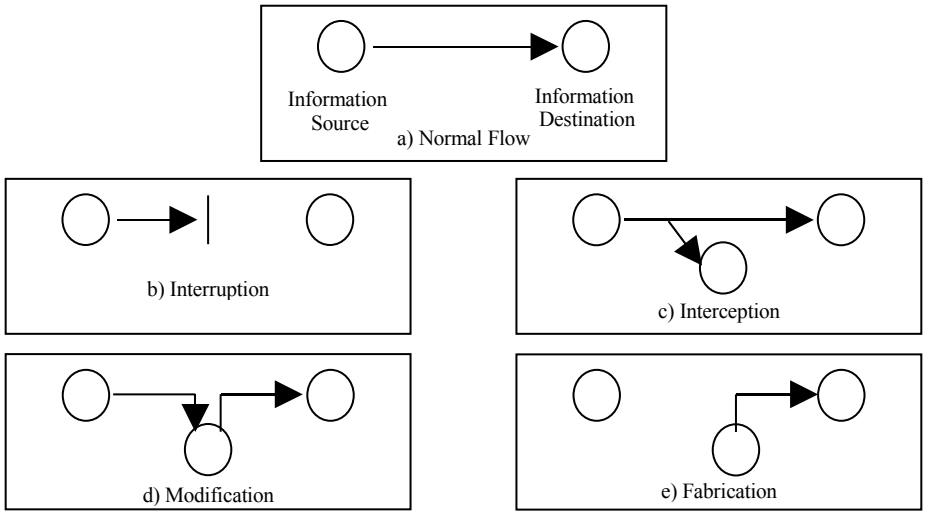

Figure 4 Security Threats According to Stallings

	Name	Sender	I Effect	Receiver
I0	Normal	100%	0%	100%
I1	Interception	100%	<=100%	100%
I2	Modification	100%	>0%	<100%
I3	Fabrication	0%	100%	100%
I4	Interruption	100%	100%	0%

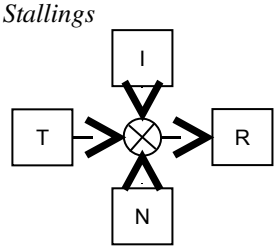

Figure 5 Interference Model for Information System

However, Stallings-type activities can be arranged in order of effect on information and message validity. For this paper, these 'interferences' (Figure 5) are defined as I0 or Normal transmission, I1, Interception, I2, Modification, I3, Fabrication and I4 as Interruption. Communication between the transmitter (T) and receiver (R) has noise (N) from all sources and intentional interference (I).

Kahn discusses the options available to the sender who may hide the message form (steganography), hide the message meaning (cryptography), hide the source and destination (traffic security) and/or hide the route taken (emission security) (Kahn, 1996, p. xviii). It is proposed that a message meeting these criteria is resistant to Stallings type activities.

Cost-Benefit

Bandwidth may be defined in terms of clock speed, data path width and efficiency (Maj and Veal, 2001, p. 2). Of note, 'Efficiency' is defined in terms of clock cycles to transfer information in bytes. This may be viewed as benefit (bits transferred) against cost (clock cycles required) where message size is affected by hardware implementations (eg pipelining), coding (eg ASCII) and communication protocols (eg RS232) with error detection/correction capabilities.

We define two parameters as 'Feasibility', an estimate however reached, and 'Efficiency' which is 'Benefit over time' divided by 'Cost over time'. Ignoring the common time coefficient, Efficiency E = b/c = benefit divided by cost. Given that difficulty may exist in determining benefit, estimates based on appropriate heuristics or operational statistics may be used.

In project management, the PERT method assesses activity duration by averaging normal, best and worst estimates. Jordan and Machefsky suggest '*The time estimate derived from a PERT chart tends to be more accurate than a best-guess estimate*'. (Jordan and Machefsky, 1989, p. 118) Extending this to group estimations, Surowiecki suggests that the average of the best guess of each group member may be more accurate than the best guess of only the fewer, smarter group members. (Surowiecki, 2004, p. xiii) However, it relies on a method of '*aggregating the information of everyone in the system*' (ibid. p. 74)

Consequently, the Estimation Table (Figure 6), based on estimates of a particular IW activity may be extended to include wider range of gradations or numeric values.

	Low Efficiency	High Efficiency
High Feasibility	Average	Good
Low Feasibility	Poor	Average

Figure 6 Estimation Table

Considering the interference modes (I0 – I4), then cost-benefit (C-B) based on feasibility and efficiency assessment may be expressed as a function of interferences, feasibilities and efficiencies. Estimation of each interference effect in a node may produce an overall estimate on which to base decisions. This estimation may be based on statistical, operations research, heuristic or other techniques selected for the task.

$$C\text{-}B_{node} = f1(\alpha_0 I_0, \alpha_1 I_1, \alpha_2 I_2, \alpha_3 I_3, \alpha_4 I_4) \text{ where } \alpha \text{ is a coefficient}$$

Further, each node estimate may aggregate all the interferences for a single figure that can be combined with other nodes for a system figure. Alternately, each node interference eg I_2, may be summed across the system to produce a system I_2 estimate.

$$C\text{-}B_{system} = f2(C\text{-}B_0, \ldots, C\text{-}B_{n-1}) \quad \text{or} \quad C\text{-}B_{\text{system Ix}} = f3(Ix_0, \ldots, Ix_{n-1})$$

The aggregation functions selected may depend on the quality of the estimates. For example, numeric estimates based on operational experience may be mathematically treated, while '*belief functions allow us to base degrees*

of belief for one question on probabilities for a related question.' (Shafer, 2000, p. 1) Alternately, arithmetic or heuristic methods may be suitable.

An overall feasibility matrix may be completed for the system model and a reasonable metric for interference may be node bandwidth. It is noted that system bandwidth measurement is complex and outside the scope of this paper.

Extending a feasibility matrix for each interference on each node with better metrics may produce numbers for analysis. For an example node, given I0 = 100% and I1 = 80%, I2 = 60%, I3 = 55% and I4 = 30%. These values may be averaged or weighted as necessary

Alternately, should exigencies proscribe certain interference modes ($\alpha_x = 0$) then the model can be recast. This numeric extension of the 'Feasibility – Efficiency' estimation was suggested by the paper on '*Attack Trees*' by Schneier (1999)

Classification

To overcome the shortcomings of Fisch and White, and Stallings, and build on the Shannon model, it is proposed that common characteristics of any IW activity are mode, means, origin, path, destination and effect (Table 1).

IW Activity Classification			
MODE	Overt/Covert	Attack visibility	Sender
MEANS	Hardware/Software/People	Attack agent(s)	
ORIGIN	Intrinsic/Extrinsic	Is it part of the targeted system?	Path
PATH	Internal/External	Is it applied internally or externally?	
DESTINATION	Hardware/Software/People	Targeted component	Receiver
EFFECT	Overt/Covert	Result visibility	

Figure 7 IW Activity Classification

While this classification does not explicitly address the time component of the activity, the feasibility and efficiency (cost benefit) estimation may provide a starting point.

Information systems components can interact, for example, people can attack people, software and hardware through activities such as assaults, hacking, theft and damage. Software attacks include identity theft, erroneous code, Trojan horse, virus, worm and Distributed Denial of Service (DDoS) attacks. All of these attacks have been documented (Hutchinson and Warren (2001); Denning (1999); Schwartau (1996)).

Schwartau discusses 'Chipping' seen as unauthorised modification to electronic components to attack a system, though research to date indicates little in general access on successful or implemented chipping operations. However, 'chipping' can be seen as an extension of traditional sabotage techniques or normal crime.

Counterfeiting expensive components or substitution of cheap components for commercial gain is not new. Further, an incident, if detected at all, may be treated as 'caveat emptor' rather than an incipient IW operation.

Counterfeiting of expensive components is prevalent (Chesterman and Lipman, 1988) and with short operational life cycles (2-4 years) of conventional computer equipment, a substandard component may not be detected unless it causes noticeable problems. For example, network interface cards (NICs) are relatively cheap and readily available, investigation into poor performance may not be financially viable.

Modification Attacks on Information Systems

Shannon and Weaver's information system model comprises information source, transmitter, receiver and destination. (McQuail and Windahl, 1981) Detectable noise, in this model, is inherent in the system, is internally applied and affects the information transferred across the system. 'Noise' may also be described as a 'modification' in that it may alter information content. Adding noise to a system may be the intentional result of electronic warfare (EW) jamming operations and may be classed as a Stallings type modification.

We propose a minor change to include additional modification sources to indicate where IW attacks may be made.

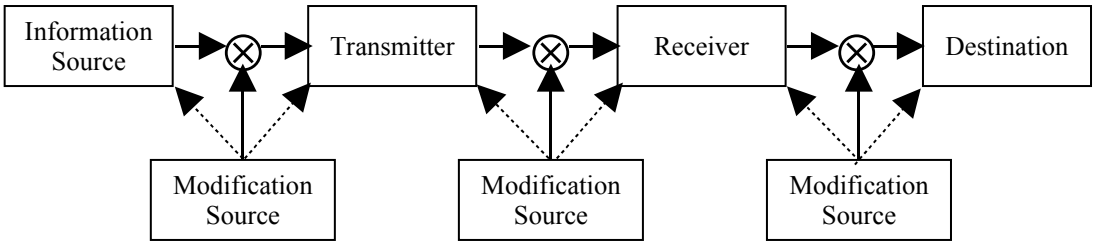

Figure 8 Shannon and Weaver Model with Additional Modification Sources

A distributed information system comprises nodes containing components; components include people, hardware and software. In a distributed system such as a public communications infrastructure, component attacks may be mere nuisance countered with technological changes and system management. For example, public phones may be replaced by mobile phones or relocated into attended public areas. Node attacks, such as a telephone exchange may be countered by backup facilities and re-routing traffic around the damaged node. System attacks require sufficient resources to mount and coordinate attacks to minimise the use of technological changes, redeployment, backup facilities or message re-routing.

A simple model such as the '*Lanchester-type combat model*' (Giordano and Weir, 1985, pp. 369-376) shows how initial resource levels and competitor efficiency interact. Given few attackers and many nodes, the attackers need to be very effective to damage enough nodes to incapacitate a system. Consequently, only node level attacks may currently be considered feasible.

In special circumstances, such as collocation in manufacture, storage or transit, 'System' attacks may be made. However, collocation increases defence efficiency with unimpeded access and concentration of resources. Further, replacement systems may be readily available.

One possible IW attack on system hardware is the use of substandard components during the construction, repair and upgrade phases of a project. The crime of counterfeiting high-value components is widespread (Chesterman and Lipman, 1988) and may include the use of substandard materials to maximise profits. Common project management methods include 'Just-In-Time' (JIT) techniques where minimal inventories depend on reliable vendor supply (Bartol and Martin, 1991, pp. 655-656). Manufacturers may use brokers for some component services but verifying component provenance may be difficult. Further, seeking compensation for direct and indirect costs of the substandard components may be difficult.

A Notional Modification Attack on a Collocated Distributed System

Given that distribution logistically complicates a system wide attack and collocation simplifies the attack but increases defender's effectiveness, a surreptitious attack may be considered. In an IW context, a system attack through substandard components may create disruption or damage but may be detected by existing Quality Management techniques (Blanchard, 2004, p. 40). Substandard components, while ostensibly for profit maximisation, may be an intentional attack on a system. However, 'pseudo-standard' components (nominally identical to normal components) may contain additional functionality. This attack is described as 'Chipping' (Schwartau 1996; Maxwell, 2004) and as a 'System Containing Unauthorised Modifications' (Shaw, 1995).

The hardware-based unauthorised modification (UM) has four phases, Replication, Introduction, Initiation and Manipulation. The software-based attack (Virus) usually requires introduction prior to replication.

Silicon foundries may provide design and construction services. A functionally equivalent design with desired modifications lawfully acquired might only need relabelling to complete replication. Consequently, we can classify this attack as a '*covert, hardware, intrinsic, internal, hardware attack with overt or covert effects'*.

Some commentators suggest that the introduction is the difficult part of the attack. (Maxwell, 2004) However, if the system operators are targeted, then a belief that an attack has occurred (overt, hardware, intrinsic, external, people, overt) may be achieved by managed detection of an UM. This may provoke the system operators into costly defensive measures to achieve the desired results. For example, additional time and resources spent dealing with normal faults may be exacerbated by the UM perception.

However, in both these cases, the storage and distribution network may provide introduction opportunities where components may be inserted or swapped in store or transit during legitimate system manufacture. Initiation may be based on system parameters such as clock cycles or event counts and manipulation may be as simple as bit inversion at irregular intervals in the system operation.

Pseudo-Standard Hardware Modification	
Replication	Plan the attack (select the targeted system, node and component)
	Design an appropriate modification
	Create sufficient instances of the modified targeted components
Introduction	Insert the modified components into the target system
Initiation	Internal eg elapsed time, logical expression
	External eg trigger event, software feature, virus
Manipulation	Disruption (interrupt or intercept) exercise interrupts, clear/set registers
	Alteration (modify or fabricate) bit inversion, failure to clear registers
	Destruction, alter feedback, blow fuses, damage circuit boards

Figure 7 Hardware Modification Process

Example of Notional Attack

A proposed train traffic control system component detects the presence of a train on a track section by detecting the wheels making contact with both tracks. Different track sections give indication of train position and speed. Using 'majority voting' for safety, three parallel components are compared and any two of three are considered to be the correct output and the dissenting output is isolated. Reliability analysis (Blanchard, 2004, p.103) may indicate that concurrent failures may be very unlikely.

If the modified chip inverts one output channel then this will be ignored. However, two channels or more failing simultaneously may produce an error accepted as valid. In some critical systems, the isolated system may receive prompt maintenance to ensure system availability but a simultaneous failure may not be rectified.

The UM attack against user confidence occurs through impeding system usage not destroying trains though this may occur. Continued safe operation may require slowing the trains to maximise driver response time and minimise damage. However, customers may find alternate transport if the trains are late, slow or considered unsafe. Further, maintenance staff may be overworked responding to any perceived irregularity with the control system. The result will be primarily economic such as lost business, reduced efficiency and increased costs. Further, public perceptions altered by a high profile failure may take a long time to correct.

Defensive Practices

Ensuring quality may become a substantial problem for all concerned in component manufacture, handling and use. It may become practical to include rigorous personnel selection, testing and licensing coupled to effective workplace policies for component storage and handling. Contractual requirements need to clearly define responsibility as well as verification and certification of design and materials. Traditional Quality Assurance techniques may be extended to ensure that hardware attacks are detected or prevented.

In addition to process changes, component records and associated information need be kept. Requirements for records management systems include written policies, training and support, system controls, access controls, system audit trails, routine and regular testing of hardware and software and adequate security. Additionally, there are Australian standards relating to record management practices. (AS15489, 2002) Further, electronic records are now readily admissible in support of legal argument. These records must be maintained in suitable manner to permit such use.

Ongoing logistic support includes reliability analysis and estimates spares requirements to maintain system reliability, however, these estimates may be insufficient to counter an UM attack. '*Major factors involved in this process are (1) the reliability of the item to be spared. (2) the quantity of items used (3) the required probability that a spare will be available when needed (4) the criticality of item application with regard to mission success, and (5) cost.'* (Blanchard, 2004, pp. 102-103) An unforeseen or unconsidered factor in the calculations may adversely affect maintenance, system serviceability and mission availability at any time during the service life.

It is noted that part of a new critical system acquisition process includes logistic support analysis to identify the necessary spare parts needed. While current storage and warehousing techniques will maintain the stock availability, the store itself may be targeted by a hardware UM attack. Additionally, these spare parts may need tamper-resistant packaging and secure storage to minimise the opportunity for tampering or theft.

These requirements may increase the cost of manufacture, transport and storage of components. Additionally, records may need to prove compliance, contest legal proceedings as well as locate the spares as needed. The Record Manager may need to demonstrate that the relevant information can be found and used for whatever purpose and that the records are reliable. This may extend to the information technology itself with management of hardware, software and associated operating information.

In time of conflict, the supply of necessary materials may require substantial facilities, information systems and intellectual property. A nation dependent on electronics may need to maintain a complete design and fabrication capability to ensure that hardware attacks are not effective.

This raises concern over 'Trusted' manufactures where products are commonly obtained from commercial sources, often based overseas. Local manufacture of desired items may breach commercial licensing and intellectual property rights. While reparations may be made after the fact, obtaining the information and infrastructure to commence manufacture may be difficult. Technology transfer may be affected by national policies on areas as disparate as education, globalisation and environment.

However, while existing policies and practices may be extended into trusted manufacture, the costs must be borne as part of the overall cost of producing or operating the system. This may adversely affect the efficiency and cost effectiveness of the system and in some cases the system will never be built.

CONCLUSION

Information system models may be used to determine system liability to attack. Attacks may be classified by source, channel and destination. Attack feasibility and efficiency estimates may be based on heuristics or empirical knowledge. An attack against operator confidence in a system may occur through using substandard components in a system. Components may be modified to produce errors in response to stimuli.

All components are modifiable at some stage and from many sources to produce an unauthorised modification with effects ranging from almost undetectable to catastrophic. Improved security in storage, transport and packaging can limit the opportunities to introduce modifications. However, costs of ensuring component quality may become a substantial problem.

Ensuring component supply for critical systems may require major investment in resources, diplomacy and business negotiations. 'Trusted' manufacture to ensure continued supply of mission critical components may be very costly if intellectual property, technology transfer and political considerations are included. These costs must be considered in the design and implementation of any critical system.

REFERENCES

AS15489 (2002) *Records Management* Standards Australia

Bartol, K.M. and Martin, D.C. (1991) *Management* McGraw-Hill ISBN 0-070-003926-7

Blanchard, B.S., (2004) *Logistics Engineering and Management* Pearson Prentice Hall

Chesterman, J. and Lipman, A. 1988. *The Electronic Pirates - DIY Crime Of The Century* Routledge, Chapman and Hall, London. ISBN 0-415-00738-0

Denning, D.E., (1999) *Information Warfare and Security*. Massachusetts: Addison-Wesley.

Fisch, E.A. and White, G.B. (2000) *Secure Computers and Networks- Analysis, Design, and Implementation*. CRC Press LLC.

Giordano, F.R. and Weir, M.D. (1985) *A First Course In Mathematical Modelling* Brooks Cole Publishing

Hutchinson, A.P.W. and Warren D.M. (2001) *Information Warfare- Corporate Attack and Defence in a Digital World.* Butterworth-Heinemann.

Ignatieff, M. (2000) *Virtual War* Chatto and Windus ISBN 070 1169435

Jordan, E.W., and Machefsky, J.J., (1989) *Systems Development* PWS-Kent

Kahn, D. (1996) *The Code-Breakers* Scribner

Kuschner, K. (1998) '*Legal and Practical Constraints on Information Warfare*' http://www.cdsar.af.mil/cc/kuschner.html accedd june 2004

Macksey, K. and Woodhouse, W. (1991) *The Penguin Encyclopedia of Modern Warfare* Viking

Mc Quail, D., and Windahl, S., (1981) *Communication Models - for the Study of Mass Communications* Longmans ISBN 0-582-2957206 LoC 80-41780

Maj, S.P., and Veal, D. (2001) '*B-Nodes: a proposed new method for modelling information system technology'* in International Conference on Computing and Information Technologies, 2001 Montclair State University New Jersey, USA

Maxwell (2004) http://www.maxwell.af.mil/au/awc/awcgate/iw-army/mod6.htm Accessed 07June2004

Schneier, B. (1999) *Attack Trees* http://www.schneier.com/paper-attacktrees-ddj-ft.html#rf8 accessed june 2006

Schwartau, W., (1996) *Information Warfare- Cyberterrorism: Protecting your Personal Security in the Digital Age.* New York: Thunder's Mouth Press.

Shafer, G. (2000) *Dempster- Shafer Theory* http://www.gallup.unm.edu/~smarandache/DSmT.htm Accessed May 2005

Shannon, C. E. (1974). *A Mathematical Theory of Communication*. In D. Slepian (Ed.), *Key Papers in the Development of Information Theory* (1st ed., pp. 5-29). New York: IEEE Press.

Shaw, D.T., (1995) *Systems Containing Unauthorised Modifications*. Unpublished Study. Edith Cowan University

Stallings, W. (1998) *Cryptography and Network Security: Principals and Practise.* 1998, Upper Saddle River, NJ: Prentice Hall.

Surowiecki, J. (2004) *The Wisdom of Crowds* Abacus Time - Warner

Taha, H.A. (1992) *Operations Research – An Introduction* 5th Edition Maxwell MacMillan International

Waller, D. (1995) "*Onward Cyber Soldiers*" in TIME Australia magazine 21AUG95 No. 33.

Waltz, E. (1998) *Information Warfare – Principles and Operations* Artech House London ISBN 0-89006-511-X LoC 98-30140

Yurcik,(1997) http://www.math.luc.edu/ethics97/papers/Yurcik.txt accessed july04

COPYRIGHT