The Case for Integrating Information Security and Intelligence courses

W. Hutchinson

School of Computer and Information Science
Edith Cowan University
Mount Lawley
Western Australia 6050
Email: w.hutchinson@ecu.edu.au

ABSTRACT

As the Western nations move further into the Information Age, the strategic nature and value of information becomes more apparent. The conventional approach to (corporate) information management, security, and its associated systems has conventionally been narrow, protective and a reactive. However, this paper argues that information security is a part of the information management (rather than the security) function, The contemporary concept of Information Warfare has developed the ideas of information both as a 'target' and a' weapon'. This means an aggressive and dynamic organisational change in the use of information and associated systems. A change in mindset is required. An integrated information strategy requires an integrated perspective on security (a protective paradigm) and intelligence (an aggressive paradigm). This paper argues that courses for information professionals of the future should integrate these worldviews in their content and objectives. A post-graduate course developed along these lines and being implemented at an Australian university will be offered as an example.

Keywords: Information warfare, information security training, intelligence training, information superiority, education.

INTRODUCTION

It is generally accepted that in the Information Age that information is the defining element in a modern organisation's competitive stance. Ideas of *information superiority* are becoming acceptable on which organisational strategy can be based. Information superiority has been the aim of commanders since the dawn of warfare. However, the contemporary concept derives from the Gulf War in the early 1990s (Campen, 1992). It involves the use of integrated electronic communications and computer networks plus the use of sophisticated satellite and airborne surveillance to totally dominate the battle-space. This is a two way process. Not only is the C4I (command, control, communication, computers and intelligence) system capable of providing better information for one's own actions, but this very advantage often allows the enemy's C4I system to be degraded. This degradation of the opponent's abilities is caused by the capability to monitor and disrupt data communication, and also to manipulate and fabricate data. Thus, the adversary knows 'what you want them to know'. This concept has also been exploited by the US in both the conflicts in Kosovo (Ignatieff, 2000) and Afghanistan. All this tends to lift the 'fog of war' (see Owens, 2000). In other words, the information confusion caused in all dynamic battlefield situations is alleviated to some degree.

Other commentators (Arquilla and Rondfeldt, 1996) have seen this trend merge with the development of networks in the organisational and societal contexts. All this is facilitated by information technology. Hence, there is also a trend for the effective use of networks in a competitive sense to diffuse from the military into commercial and government organisations.

A simple version found in Alberts *et al* (1999), and Alberts and Gartska (2000) defines information superiority in terms of timeliness, relevance, and accuracy of the information supplied to the commander (manager). Coupled with this, is the assumption that the information is given to the correct manager, is in an easily comprehensible form, and that the manager acts effectively on the information presented in a timely fashion. In conventional, contemporary organisations these concepts are relevant where forms of competition are in play. Hence, it is relevant to almost all organisation and certainly competitive, commercial businesses.

All this discussion of information superiority begs the question: what is information? It is in this definition that lies the basis for a modern and rational approach to information management education. The conventional linear definitions of data, information, knowledge, and wisdom with each stage having a greater degree of collation and involvement with context and learning does not appear to be very useful. In fact, this definition appears to delineate many functions such as knowledge management, information management, and, in the author's opinion, propagates confusion around these roles. What is needed is a definition that reflects the integrated nature of the *information* security function. One such definition of data, information, and knowledge was developed from Boisot (1998) - see Hutchinson and Warren (2001a, 2001b). In his model, data is associated with a *thing*, and discriminates between different states of the thing it describes. It consists of attributes of the events or objects it describes. On the other hand, knowledge is an attribute of an *agent*. Knowledge is a set of interacting mindsets about data activated by an event. Hence, in most circumstances the word ‘agent’ means a human being or a group of people. Information is the set of data filtered by the agent within the bounds of the knowledge held by the agent. It establishes a link between the agent and the data. Information is a 'product' of human cognition (knowledge) and its interaction with the environment (data).

Hence, the foundations for 'information education' lies in these new definitions of information and information superiority.

THE PRESENT SITUATION

The definitions given above imply three major things:

- In a modern organisation all functions (including the Information Security function) should be dynamically assisting the organisation to achieve information superiority
- The information security function is about human and data management (and their associated communication, storage and processing technologies), and
- The definition of 'information' used above is more akin to the conventional meaning of 'intelligence'.

However, the present practice of information security education concentrates more on the passive defence of data. Humans are included in topics such as 'vetting' but are generally excluded. Information security is lumped in with the general security functions and with physical and building security. It is often confused with computer or network security. Hence, in many organisations, it is the province of the technician. It is an 'add on' to the real business of the organisation. Thus, it becomes marginalised from what are regarded as the core business activities much as information technology (IT) was in the 1970's and 1980's when IT and its staff were regarded and as a necessary evil, but not a true **business** function. In the Information Age, this can be a fatal mistake not only for the organisation but for information security professionals as well.

The ideas above are encompassed in the recent acceptance of the notion of 'information warfare'. This has both in its offensive and defensive (security) modes and is closely aligned with information superiority. This is has been well documented by authors such as Schwartau (1996), Knetch (1996), Denning (1999), Waltz (1998), Hutchinson and Warren (2001), and Jones *et al* (2002). Thus, information security professionals should recognise the information warfare paradigm and become an integral part of the organisation's business and not peripheral to it. If this accepted then training for Information Security courses should be revamped to give professional a grasp of the overall **use** and **protection** of information within an organisation. Information security has links with other forms of security but is fundamentally different in that it should be associated with information and general management rather than the more technical areas of IT and physical security.

If the flow of information within an organisation is examined (see figure 1) then the enormity of the information security task can be seen. Information is derived and disseminated both internally between operational units and management, as well as the external environment by environmental scanning and releasing data to the environment by perception management practices (and, in unmanaged ways by accident or default). An integrated information process is needed to manage the integrity of data/information flow both to and from the external world as well as the internal realm. This substantially broadens the role of information security into the realm of intelligence. One cannot be fully understood without the other. The reactive security world merges now with the proactive intelligence domain. The author argues that this concept should be the basis of general Information Security (as well as Intelligence) education. From the ideas of offensive and defensive modes of operation, the topics that need to be considered can be included (see figure 2) in the curriculum. Thus, the course will enable the student to develop skills necessary for the dynamic 21st century organisations, rather than the passive, *Maginot Line* paradigm of conventional security practice.

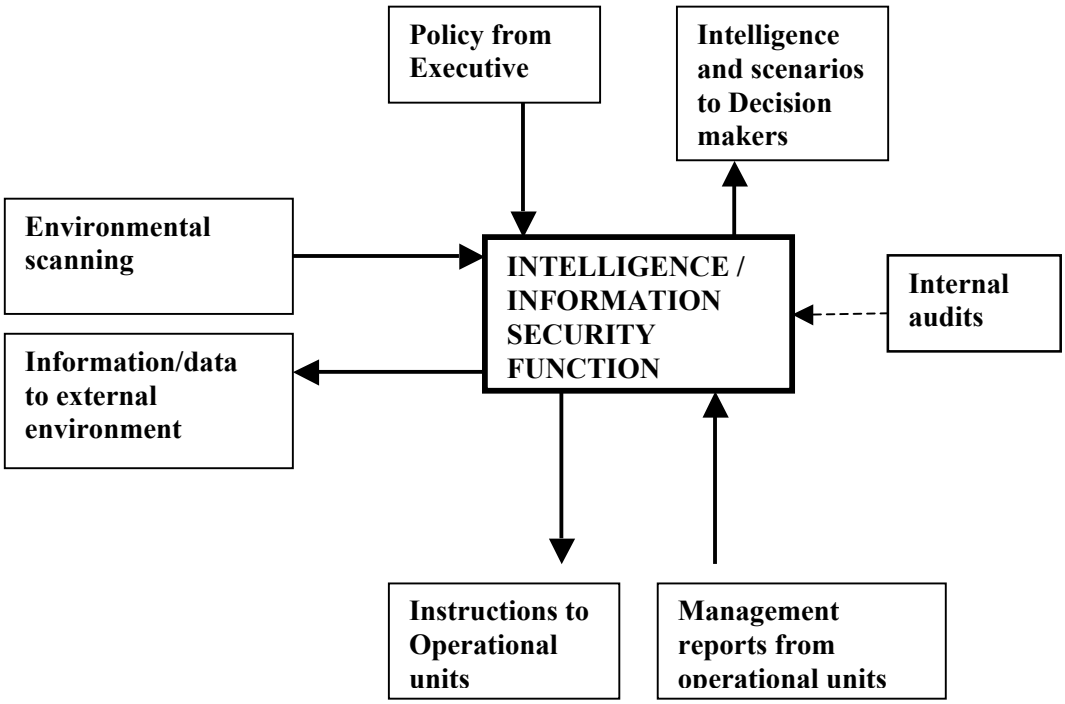

Figure 1: A simplification of data/information flow in a organisation (based loosely on a model developed by Beer, 1984. 1985)

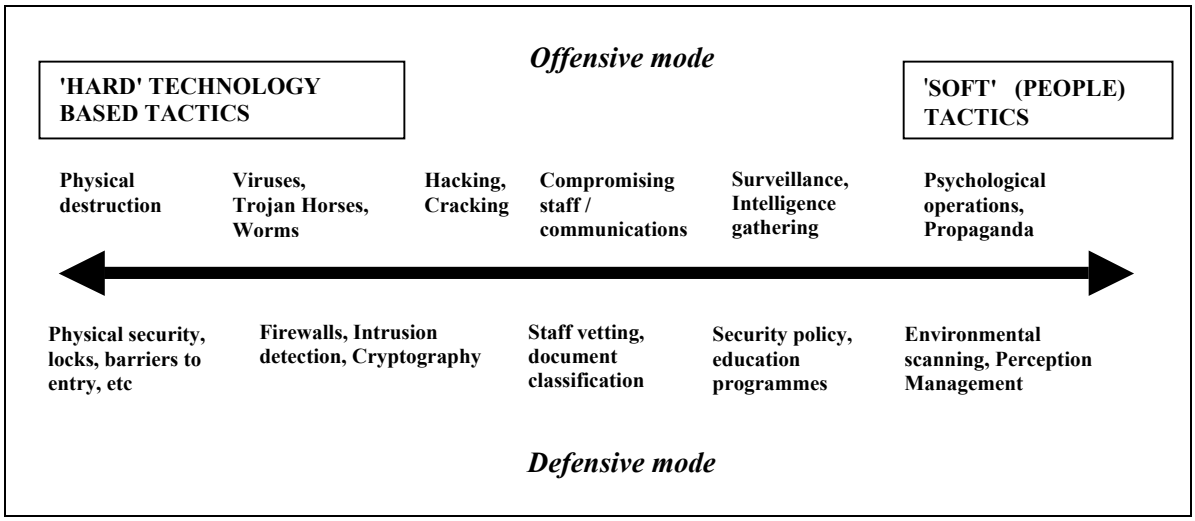

Figure 2: Examples of the range of topics involved in the concept of information security (author)

Corkhill (2002) gives a real world example of a similar approach taken in industry. The company in question mines and processes diamonds. In this company:

> *"Security intelligence plays various roles within the corporate sector. An effective program operates at both tactical and strategic levels and supports the business in both defensive and offensive roles. Defensive roles includes supporting the*

company security strategy in terms of physical, personnel, and information security. Offensive roles are in support of the company business strategy."
(*ibid,* p.14)

Whilst this function now incorporates the entire security function (rather than just information security) and the intelligence function, it shows how a dynamic business role has been created.

AN EXAMPLE OF AN IMPLEMENTED POST GRADUATE CURRICULUM

As these ideas were being developed, it was decided that the courses at Edith Cowan University in Western Australia would be redesigned. At the undergraduate level, there are a number of units within a computer security minor covering computer, information, database and network security. Until 2002, this was the case with postgraduate offerings. It was decided that a course embracing the ideas above was need as well as the more technically oriented computer security courses. A coursework Masters level course was created to cope with that perceived market need. It specialises in network and computer security plus more specific topics such as wireless security and forensic computing. A new Masters course focusing on information security and intelligence was created to develop skills in the 'information warfare' paradigm. The underlying thoughts behind this were based on the assumption that organisations would need people who understood the true nature of information and its roles as a 'weapon' and a 'target'.

This initiative was taken by the School of Computer and Information Science within the university, but was intended to be a multi-school, interdisciplinary course.

The course had to include all the elements included in the Boisot based model: data, knowledge/context, and information. In order, these mapped into:

- **Data**: conventional computer/network, information security
- **Knowledge/context**: perception management
- **Information**: intelligence

These elements had to be held together with a 'general' unit on information warfare that brought the areas together. The Boisot model was emphasised in each of the units especially the first introductory subjects. The initial Information Warfare unit introduced the unity of all these elements in an organisational sense. The advanced Information Security unit also integrated the subjects. (This unit should really have been named Advanced Information Warfare). Treating 'information security' as a proactive and dynamic activity was thought to make it more relevant to organisations and bring it more into the mainstream business, rather than a marginalised function regarded as a cost. Information Security became a value added business role.

The course developed is a postgraduate offering in Information Security and Intelligence and is available in on-campus mode or fully on-line. It consists of three stages: Graduate Certificate, Graduate Diploma, and Professional Masters. Entry requirements are an undergraduate degree or five years appropriate work experience. Table 1 shows the composition of the units for each stage. The complete course takes 18 months full time or an equivalent part time load.

The compulsory content gives the student the range of technical skills required in a technological environment as the softer management and psychological aspects of information security. The elective content gives the participant the ability to either take a

range of units in the area, or concentrate on a specialist area such as computer/network security. As it was originally designed as a course work Masters, Stage 3 originally consisted of three, advanced specialist units. However, a number of prospective students expressed a desire to either complete work-based projects or research. The option was then added to allow students to complete a work or research related project instead of the final three advanced units. This is now the School's favoured option.

Compulsory units	Elective units
Stage 1: Graduate Certificate Information Security *(a conventional information security unit covering the defensive function of security)* Introduction to Information Warfare *(a general unit integrating all the elements in the Boisot model)*	***Take any 2 units from:*** *Technology based units* Database Security Computer Security Introduction to Knowledge Management The Information Society Fundamentals of Cyber-crime Physical Security *Social/human related untis* Media and Advertising*)* Media and Nation Global Communications Introduction to Media and Communication
Stage 2 - Graduate Diploma Contemporary Intelligence *(covering the information/intelligence aspects of the Boisot model)* Perception Management *(covering the knowledge/context aspects of the Boisot model)* Information Security *(covering a continuation of the both the lower level Information Security and Information Warfare units, integrating them both)*	
Stage 3 - Masters Research project (3 units) **OR** ***any three Advanced from:*** *Technically oriented units* Computer Security Network Security Database Security *Social/human oriented units* Media and Social Issues Ethics, Values and Moral Decision Making Current Issues in Security Advanced Security Risk Management Advances in Security Technology	

Table 1: The break up of units for Information Security and Intelligence awards

In stage 1, the compulsory units cover both the defensive ('Information Security') and offensive ('Introduction to Information Warfare') aspects of the area. The two elective units allow the student to complete two specialist units from the hard and soft spectrum of topics. Stage 2 covers the range of topics within the intelligence function. The units cover advance Information Security (from both defensive and offensive perspective), the psychological impacts of information usage ('Perception Management'), and the principles of intelligence and counter-intelligence ('Contemporary Intelligence'). Stage 3 then allows a student to do further research in a topic of interest, or take advanced subject units.

The main, desired graduate attributes from this course (apart from content knowledge and computing skills) are in the cognitive realm. Each unit has its own stated objectives but overall the student should develop skills in observation, analytic and forensic skills, inductive and deductive reasoning, and lateral thinking.

Also, there is a requirement to set information security in a social, ethical, political, and organisational context. These are achieved by a number of exercises such as:

- forensic computing (for example: analysis of log files)
- case studies (analysis of situations)
- 'thinking like the enemy' exercises (students will have to justify the position of the enemy, etc.)
- debates (students will debate contentious subjects such as staff surveillance, biometrics, privacy, etc.)
- conclusion exercises (students given scant information and asked to come up with scenario to expose hidden assumptions)
- scenario exercises (role playing in situations)
- lateral thinking exercises
- observation exercises

Basically, the student will have to have the skills to think both like an attacker and a defender, and make decisions whilst considering the social, ethical, organisational, and legal context of the problem. Importantly, the dynamic and critical role of information in the modern organisation should be fully grasped. It is understood that due to time constraints many areas of relevant study, such as information theory, are not covered well. However, it is argued that the course is an appropriate grounding for roles such as Chief Information Officer (CIO), rather than a Chief Data Officer or Chief technology Officer which many CIOs are in reality if not in name.

CONCLUSION

The development of the information warfare paradigm is still in its early stages. The overall success of this venture has yet to be determined as there have been no graduates; the course starting in mid-2002. There has been much interest from industry, intelligence related government departments, the military, law enforcement, and even local government. The present student cohort comes from the finance industry, law enforcement, military related private industry, and local government. The course's effectiveness will be monitored and be fine-tuned to accommodate any shortcomings.

The approach described above takes a different tactic to information security making it a part of the overall intelligence role within an organisation rather than the closely related security function. It is based on the assumption that the exploitation and protection of information (hence, knowledge and data) cannot be separated.

REFERENCES

Alberts, D.S. and Garstka, J. (2000) Information Superiority and Network Centric Warfare, talk given at *InfoWarCon2000*, Washington, September, 2000.

Alberts, D.S. and Garstka, J..J., Stein, F.P. (1999) *Network Centric Warfare*, CCRP, Washington.

Arquilla, J. and Ronfeldt, D. (1996) *The Advent of Netwar,* RAND, Santa Monica.

Beer, S. (1984). The Viable System Model: its provenance, development, methodology and pathology. In*,* Espejo R, Harnden R.(eds.), *The Viable System Model,* John Wiley & Sons, Chichester. pp.211-270.

Beer, S. (1985). *Diagnosing the System for Organisations*. Wiley, Chichester.

Boisot, M.H. (1998) *Knowledge Assets*. Oxford University Press, Oxford.

Campen, A.D. (ed) (1992) *The First Information War*, AFCEA International Press, Fairfax.

Corkhill, J (2002) Blood Diamonds and Black Diamonds - the Role of Security Intelligence in the Security Intelligence in the Corporate Environment, *AIPIO News*, **35**:14-17, November 2002, Australian Institute of Professional Intelligence Officers, Canberra.

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

Hutchinson, W.E., Warren, M.J. (2001a) *Information Warfare: Corporate Attack and Defence in the Digital Age*, Butterworth-Heineman, Oxford.

Hutchinson, W., Warren, M. (2001b) Principles of Information Warfare, *Journal of Information Warfare*, **1**,1: 1-6.

Ignatieff, M. (2000) *Virtual war*, Chatto and Windus, London.

Jones, A., Kovacich, G. L., Luzwick, P.G. (2002) *Global Information Warfare*, Auerbach, Washington

Knecht, R.J. (1996) Thoughts About Information Warfare*,* in: Campen, A.D., Dearth, D.H., Thomas Godden, R (eds) *Cyberwar: Security, Strategy, and Conflict in the Information Age*,. AFCEA International Press, Fairfax.

Owens, B (2000) *Lifting the Fog of War*, FSG, New York.

Schwartau, W. (1996). *Information Warfare – second edition,* Thunder's Mouth Press, New York.

Waltz, E. (1998) *Information Warfare – Principles and Operations*. Artech House, Norwood.