2005

Seeking information superiority: Strategies for business in the commercial application of information operations

Martin Dart
Edith Cowan University

Dart, M. (2005). Seeking information superiority: Strategies for business in the commercial application of information operations. In *Proceedings of 3rd Australian Information Security Management Conference* (pp. 11-19). Edith Cowan University. Available here

Seeking information superiority: strategies for business in the commercial application of information operations

Martin Dart
School of Computer and Information Science
Edith Cowan University, Perth, Western Australia
mdart@student.ecu.edu.au

Abstract

Information superiority is a condition that many businesses attempt to attain without truly understanding what it is, or how to get there. This paper presents an overview to help businesspeople recognize the road to information superiority, and some of the essential strategies to implement along the way. Information operations is a concept described to enable information superiority, when used with a network form of organization (as opposed to simply being networked). This paper describes information operations across their fundamental structure of intelligence, surveillance, and reconnaissance (ISR); and suggests a separation between industrial espionage and legitimate business information gathering. A model for establishing information superiority is presented, outlining the importance of 'cradle-to-grave' implementation throughout the business lifecycle. This brings together key doctrinal points from the information security, information operations and information warfare fields. Supplementary material is drawn from sociology, risk analysis, and business management theory to complete the applicability of the text to business readers.

Keywords

Information superiority, information value, intelligence, surveillance, and reconnaissance, information operations, industrial espionage

INTRODUCTION

Information warfare (IW) and its related activities of information operations (IO) and intelligence, surveillance, and reconnaissance (ISR) are not just restricted to the military arena. As the power and usability of information technology has progressively permeated society it has provided private citizens, commercial entities, and other political or ad-hoc organizations with a new platform for operations, influence, and attack (Armistead, 2004).

While much of the published IW, IO, and ISR material focuses on military models and modes of conflict, there is much that is relevant to commercial practitioners. Non-military readers may however find it frustrating to translate and adapt this material to the business world, and there is further work to be done in redefining the topic so that these techniques might contribute towards achieving information superiority (IS) in commercial marketplaces.

This paper will focus on describing a new breed of business organization; one that recognizes the importance of information superiority, and uses ISR empowered information operations in a networked environment to obtain it. It will describe these issues using a perspective and language appropriate to the modern business environment.

Information superiority in the business context

While some commercial operators may feel that they are indeed at war in certain markets, for many others there is a familiarity with their business activities that makes them appear a long way from obvious adversarialism. Yet many every-day business activities are acts designed to attain information superiority in the marketplace, such as:

Purchasing an enhanced listing in a business directory

Conducting a customer satisfaction survey

Upgrading office-based computer systems

These activities all exist within a series of converging spheres that define the field of information superiority, as shown in Figure 1.

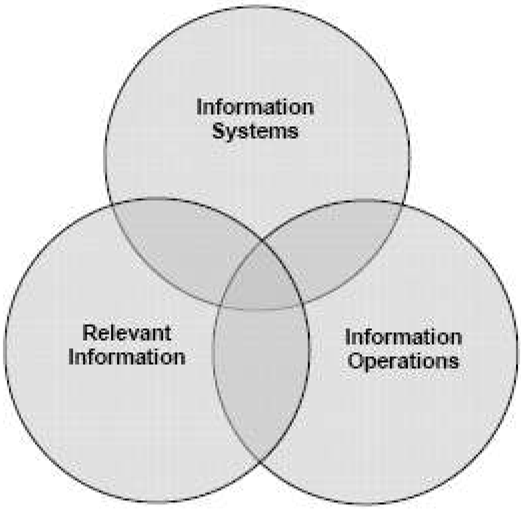

Figure 1: Components of Information Superiority

(Armistead, 2004)

It is easy to recognize and apply this model to virtually any business in any competitive arena, with examples within each sphere that might include:

Information Systems:
Email
E-business web portal
Data warehousing

Relevant information:
Stock/commodity prices
Customer demographic data
Profit margins on goods and services sold or produced

Information Operations:
False job advertising
Media relations
Enumerating competitors pricing or product offerings

The key to information superiority for any business is to achieve and maintain their competitive advantage as close to the absolute centre of this model as possible, where the benefits of proximity and interaction between each sphere of operation can be exploited. Yet in order to consolidate ones own position at the centre of the model it is necessary to dislodge others; in fact there is room for only one organization at the true centre of such a model, and all others must suffer some degree of displacement.

This competitive element underlies the basic premise and definition of information superiority, as one organization can only claim such superiority over another as a *relative* measure (Waltz, 1998). Information superiority can therefore be defined as:

> The degree of dominance that allows… the ability to collect, control, exploit, and defend information without effective opposition
>
> (U.S.A.F 1998)

In the process of obtaining such an advantage one actor must exploit its information in a way that others cannot, and may indeed actively seek to prevent others from understanding, gathering, accessing, or acting on their own information resources (Schwartau, 1996). Figure 2 demonstrates a scenario where one actor achieves information superiority over other actors by effective operations across all three information superiority domains.

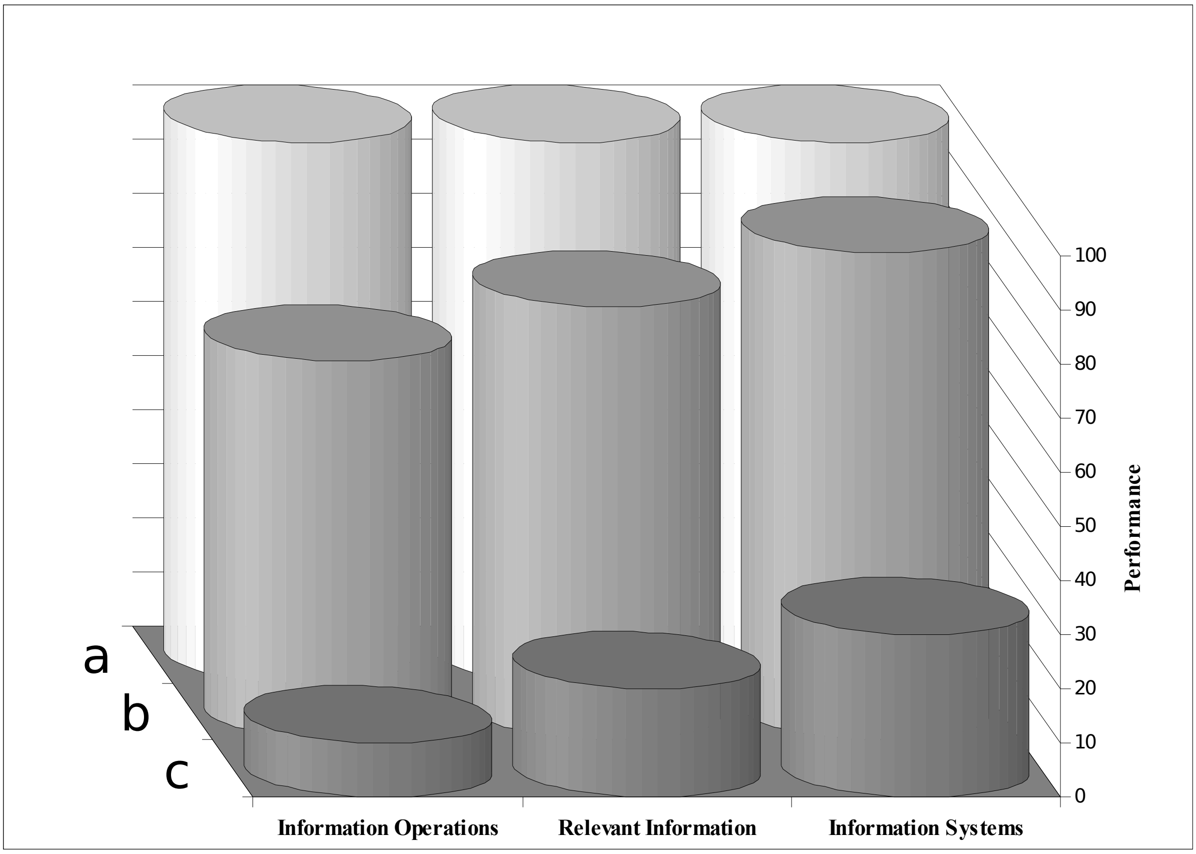

Figure 2: Relative Information Superiority positioning by actors

Shaping the Business Battlespace

As marketplaces become increasingly competitive and actors more aggressive in their quest for information superiority, then the framework within which that marketplace operates will lose the idealised symmetry shown in Figure 1. The introduction of new technologies and business practices may lead to integrations and transformations between various aspects of operation. A company that fails to maintain an effective presence in these reconfigured arenas will find itself increasingly subject to the strategic planning of the dominant actor, who therefore operates from a position of information superiority over them.

Figure 3 illustrates how the integration of information systems and relevant information can create such an asymmetrical marketplace. This scenario would result from an industry in which so much data is generated that an information system becomes essential for the processing of it. Information relevancy and information systems are therefore dependent upon each other and merge into a powerful super-domain that redefines the marketplace. The dominance of any one actor in this newly evolved domain can have adverse effects on other actors as they endeavour to implement their information operations, for example by:

Controlling access to the relevant information through commissioning it and keeping the results private
Acquiring control of either the information systems or information producers, such as by merging with or acquiring a software development or market research company.
Undertaking action within the information operations field that dissuades or prevents other actors from attacking the dominant actors position; for example by publicising a (usually non-technical) capability that customers highly value and competitors can’t match (Gartner, 2004).

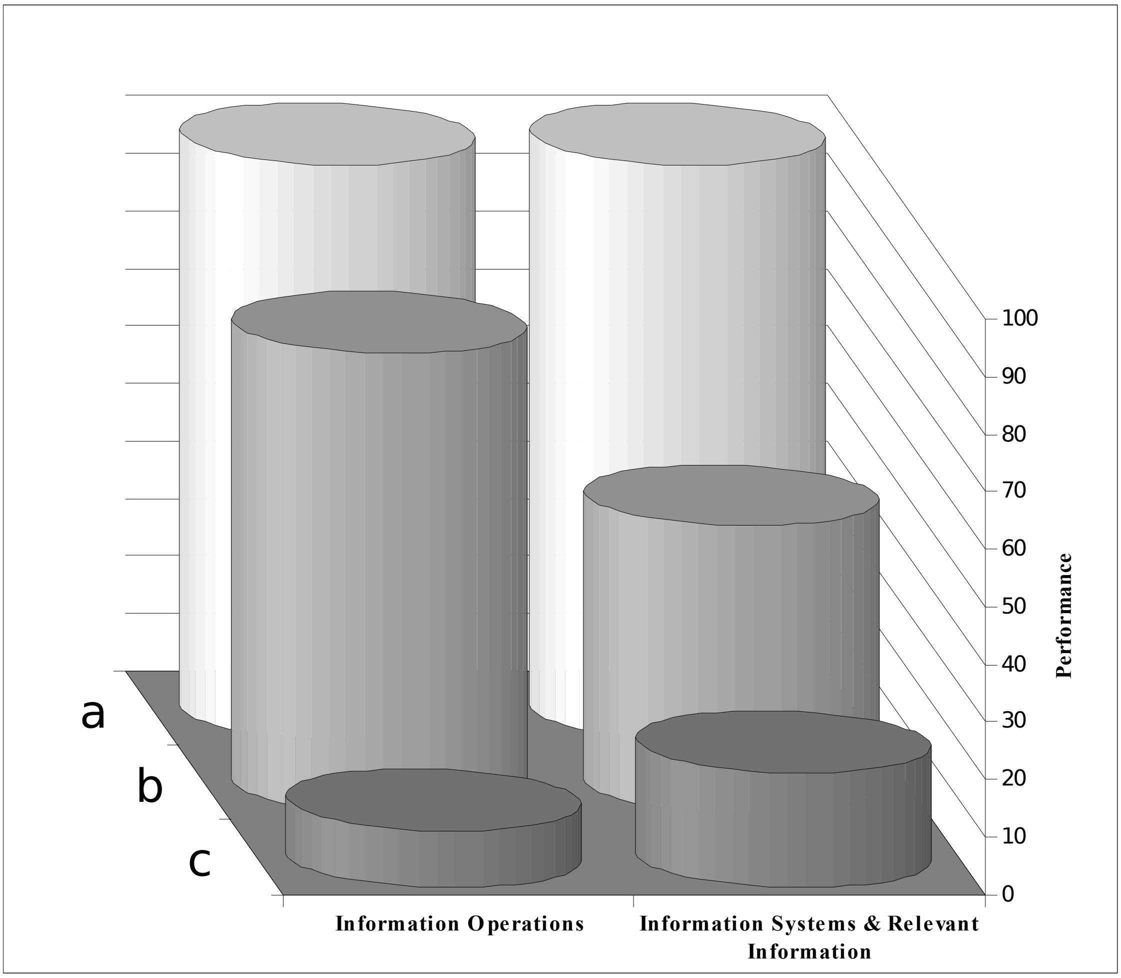

Figure 3: Shaping the marketplace to ensure Information Superiority

The scenario presented in Figure 3 tends to evolve within markets as a result of deliberate action, as opposed to accidental or fortuitous circumstance (Webster, 1995). In this figure actor 'a' has forced a market lead by merging its incoming stream of highly relevant information to a powerful information system. This has given it a significantly greater advantage than simply relying on dominance across the previously existing three separate domains, as its competitors cannot obtain the equivalent relevance of information in their systems (as 'a' has taken steps to prevent this by conducting private research). This has magnified the value and effectiveness of both the information and the system it is stored and processed in.

It is due to such deliberate action by one or more actors that new technologies gain prominence, and while the introduction of such a strategy may be time consuming, expensive, and difficult, if done well it can contribute to a position that other actors might find difficult to challenge for some time to come (Armistead, 2004). What should also be accepted into the corporate strategy is that marketplaces are constantly in this state of flux, and no single strategy is going to suit market conditions all of the time. The more actors there are in a particular marketplace the rougher the swell is likely to be from competing technologies, skills shortages, legislation, and the offensive/defensive information operations of others. In this environment the actor seeking information superiority must be prepared to change quickly (and often) the way in which they do business, and may even need to undertake all-out information warfare to protect their interests.

In military terms such posturing would be known as 'intelligence preparation of the battlespace' (IPB), and as the name implies there are intelligence operations as precursors that must take place to aid the success of subsequent action (FAS, accessed 7/4/2005, Armistead, 2004 and Waltz, 1998). Just as military planners will not undertake wartime action until sufficient information regarding the battlefield is obtained (and communications are in place to attack it with improved chances of success), neither should a commercial actor attempt to enter or control a market until they are fully aware of the potential difficulties and likelihood of conflict.

In the business world this process should be viewed as marketplace awareness and influence (MAI). MAI is composed of legitimate business activities that include:

Surveillance (of market competitors, laws, clients, or political influences)
Planning (strategic product or service direction, risk analysis, and internal audit)
Establishing communications systems
Establishing warning systems (to improve detection & reaction responses)
Provisional information operations to begin proactively gathering relevant data to map the market, undertake marketing, and develop competitive strategies.

Accepting Information Operations as an Organizational Norm

The previous examples describe what happens quite naturally in Western, capitalist economies – where competition and 'winning' is a key, often subconscious process which all actors engage in to better their position in the marketplace. Yet, as we frequently witness, this process produces numerous losers - victims of the information superiority and effective information operations of others.

However, once an organization recognizes through MAI the wider battleground within which it operates, then it is better placed to survive and prosper. The application of information superiority principles needs to be applied to *all* of its on-going activities, as information superiority is not achieved by any one department, person, product, or action. Neither is it a strategy that should be attempted only in times of increased competition or financial difficulties. Figure 4 describes a series of parallel and linear strategic processes, which would contribute towards information superiority were they to be applied from the inception of a business (or business process) and throughout the various stages in its lifecycle.

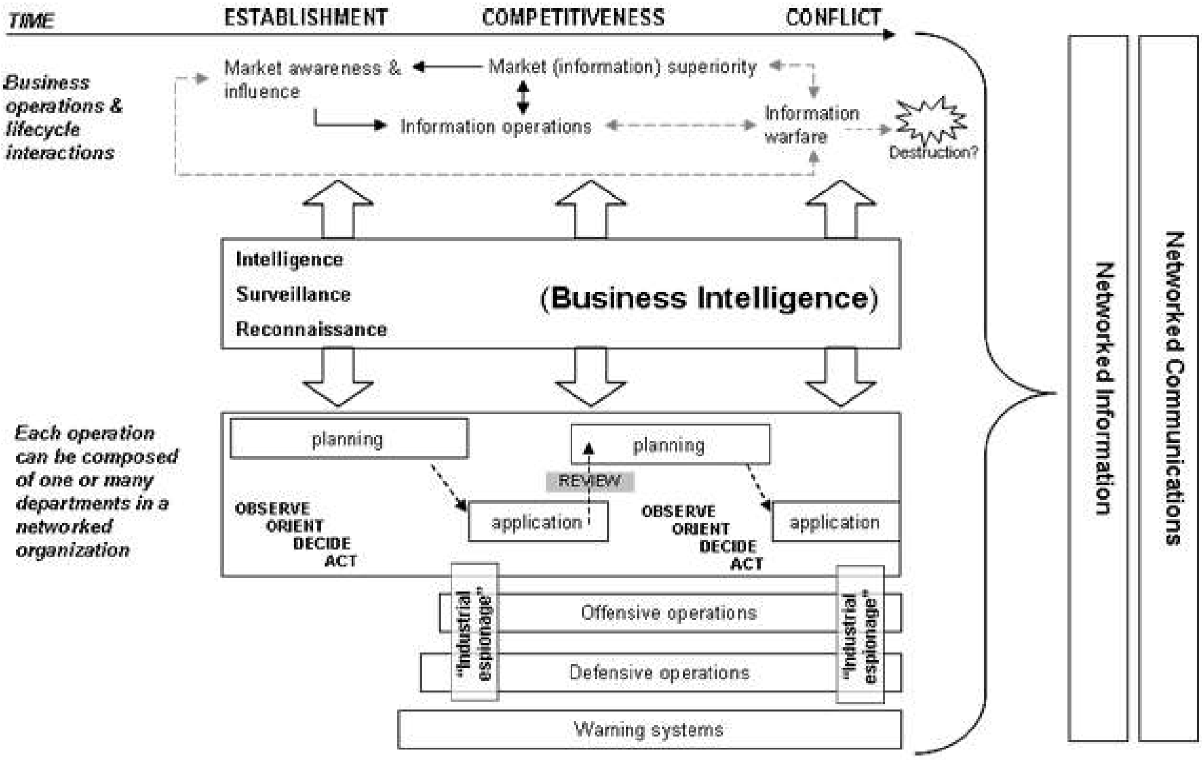

Figure 4: Business processes enabling information superiority (Author, 2005)

In order to implement such a model an organization must:
Adopt a networked structure
Operate with speed, utilizing effective offensive/defensive tactics based on observation, orientation, decision, and action (OODA) loops (Waltz, 1998)
Implement efficient information collection, management, and dissemination systems
Undertake pro-active intelligence, surveillance, and reconnaissance operations (ISR), and integrate these into all other information operations

These tactics should help achieve the twin goals of dominant marketplace awareness (DMA) and dominant marketplace knowledge (DMK). DMA is assisted by gathering data inputs from automated and human sensors in and around the marketplace, and the understanding, analysis, and application of these contributes to DMK (Waltz, 1998).

Once DMA and DMK have been attained it is possible for a business to act with confidence, maintaining knowledge of the likely response from competitors and the ability of those competitors to survive a hostile engagement. In both DMA and DMK the concepts of OODA loops should be applied, and efforts made to interrupt the OODA loops of other actors to gain information superiority over them. If just one aspect of OODA can be manipulated or removed from an opponent then their loop will crash or be corrupted, as it is a feature of OODA that if one component is removed then the loop must return to the initial 'observe' status and all subsequent actions re-tried. Business processes are disrupted if they are unable to effectively complete any OODA loops, particularly if the first two components (observe and orient) are targeted (Vacca, 2002). In such a case the informationally superior organization gains a greater prize: an attainment of the 'knowledge edge' and decision making superiority (Armistead, 2004).

Intelligence, Surveillance, and Reconnaissance

ISR are an important trio of activities for any business to undertake. ISR must be both external and internal to the organization in order to detect emerging threats and trends that can undermine not just competitiveness, but the core ability to operate and function at all. While these terms originate from the military, their translation into the commercial world has not been particularly encouraging. Often referred to as 'industrial espionage', ISR in the business arena retains an air of illegality and unfairness.

This is an attitude that must change within any organization hoping to achieve and maintain a fully-rounded position of information superiority. With this in mind it is far better to import terminology from the IT sector, and ISR for commercial organizations should be seen as simply another part of 'business intelligence' (BI) (Simovits & Forsberg, 1997). Industrial espionage will still retain a place in the taxonomy of information operations, but it should be put in its rightful position as an extreme tool for information warfare (a separate activity from normal information operations (Armistead, 2004)).

Industrial espionage is an activity used to great effect by foreign actors to acquire technology they could never develop independently, and it remains of particular danger to internationally operating corporations (Schwartau, 1996). Yet however useful industrial espionage may be as an IS/IW weapon, its use must be carefully considered due to the grave consequences of discovery, which may disastrously harm the business employing it.

Some examples of what constitutes industrial espionage are detailed in Table 1. Also included are BI gathering activities which should be considered legitimate, legal, and useful.

Industrial Espionage	Business Intelligence gathering/intelligence operations
Stealing documents from a competitors premises	Gathering from open source intelligence – news, websites ('Google hacking'), reports, patents
Hacking into computer systems and viewing/changing/removing data	Discussions with former employees of competitors
Blackmail/extortion	Hiring a 3rd party private investigator to evaluate competitors premises, business, or personnel
Bomb threats/triggering fire alarms or smoke detectors	Placing a mole in competitors organization to observe working practices
Vandalism or destruction of premises or employee cars/possessions	Dumpster diving (but avoiding trespass)
Committing fraud, other crime, or ordering goods in the name of the competitor	Mapping a competitors business links – suppliers, partners, divisions, etc
Creating and sending viruses or Trojans into the competitors information system	Listening for employee conversations in public locations – food hall, café, smokers area outside building
Making a claim to authorities of a business transgression or crime being committed by competitor (this COULD be illegal depending on nature of accusation and how you present 'evidence')	

Table 1: Industrial Espionage versus Business Intelligence activities (Robinson, 2003 and Simovits & Forsberg, 1997, and Winkler, accessed 2005).

As many businesses already possess BI software, designed to move data between departments and help interpret meaning, this should be used to provide a framework to enable the organization to incorporate ISR information and empower the all-important networked form of operation. But BI systems are only as good as the quality and diversity of information input to them, so for a BI system to contribute towards information superiority it should extend its appetite for data (using the legal techniques from Table 1) into competing organizations, consumer lifestyle habits, and legislative structures. The result for the host organization will be an ability to see the structures that exist behind the raw information, and the phenomena that influences them (Webster, 1995). With this kind of system pervading the nodes of an organization (flowing freely across departments in a non-hierarchical manner), information superiority relative to other actors in the same marketplace is enabled.

Information Value

All information in a business has value, which can range from ‘none’ to ‘essential’. As modern companies generate and process ever-growing volumes of data, it becomes vital that essential information is readily identified and utilized, and that value-less information is disposed of or stored so as not to cause a distraction. This concept of value is critical to attaining information superiority, as there has to exist a framework for prioritizing which information to either attack or defend, and this will vary depending on the marketplace and actors involved (Rues, 2003).

The value of information is increased, and its dissemination enhanced, by the use of business networks. The greater the number of nodes that can access and process information at any one time, the more new information can be generated to describe the original data, provide new interpretations, or give birth to new analysis. The simple formula which describes this phenomenon is called Metcalf’s Law, and is articulated as:

$$N*(N-1)$$

Where N is the total number of nodes in a network, and the result is a value metric based on the total amount of connectivity in that network.

While this formula holds true if we assume that all information has the same initial value and that all nodes process it in the same way to produce regular and consistent outputs, the results can be anomalous if this is not the case (Alberts et al, 2000). If we wish to accurately weight the value of information then a user must arrive at a shortlist of values that are important to them, and use the network to enhance these values above others. The establishment of such value systems will vary across marketplaces, and should be revisited regularly to establish the impact of competitive practices, intelligence operations, and network upgrades.

Figure 5 demonstrates the application of a user-generated value system, to evaluate the effectiveness of traditional retail grocery shopping against a 24x7 on-line ordering and home delivery alternative. The networked form of retailing can be identified as more effective across the spectrum of important measures for this sector.

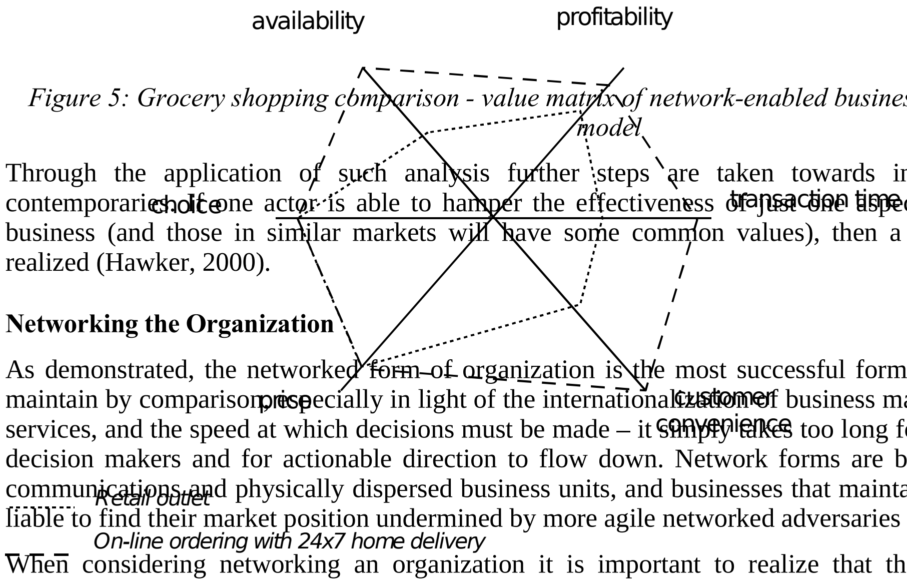

Figure 5: Grocery shopping comparison - value matrix of network-enabled business model versus traditional model

Through the application of such analysis further steps are taken towards information superiority over contemporaries. If one actor is able to hamper the effectiveness of just one aspect of value in a competitors business (and those in similar markets will have some common values), then a business advantage will be realized (Hawker, 2000).

Networking the Organization

As demonstrated, the networked form of organization is the most successful form. Hierarchies are difficult to maintain by comparison, especially in light of the internationalization of business markets, the rise of contracting services, and the speed at which decisions must be made – it simply takes too long for information to move up to decision makers and for actionable direction to flow down. Network forms are best able to exploit real-time communications and physically dispersed business units, and businesses that maintain traditional hierarchies are liable to find their market position undermined by more agile networked adversaries (Arquilla & Ronfeldt, 1997).

When considering networking an organization it is important to realize that the network must be applied internally to the organization – it is not enough to make an essentially hierarchical organization part of someone else’s network without reflecting that change within. Once the internal change has been made then extra value may be added by interfacing to other networks as the operational need arises.

CONCLUSION

It is clear that information superiority for any organization is not easy, and is not something which can be attained and then considered owned. In markets where monolithic organizations have previously prospered, network forms are taking advantage of the global availability of cheap labour, ubiquitous communications, and relaxing political barriers. Such organizations may have headquarters in one country, manufacturing in another, raw materials from several more, and a target market in any combination of all of them.

Businesses must recognise such threats early on and be willing and creative in their actions to counter them. Information superiority is a status which will enable this to happen, and in the process prevent one of two disastrous events from occurring: either all-out information warfare (which may cause damage to the marketplace and destroy the unprepared), or the knockout sucker-punch which the business just did not see coming and which undermines their information position. The time for businesses to begin their efforts toward attaining information superiority is now, and the place is here.

REFERENCES

Alberts, D., Garstka, J. and Stein, F. (2000) Network Centric Warfare: Developing and Leveraging Information Superiority, CCRP

Armistead, L. (2004) Information Operations: Warfare and the Hard Reality of Soft Power, Brassey's

Arquilla, J. and Ronfeldt, D. (1997) In Athena's Camp: Preparing For Conflict in the Information Age, RAND

FAS, Army Science & Technology Master Plan, 1997, URL http://www.fas.org/man/dod-101/army/docs/astmp/c2/P2C2.htm#II20, Accessed 7/4/2005

Hawker, A. (2000) Security and Control in Information Systems - A Guide for Business and Accounting, Routledge

Robinson, S. (2003) Corporate Espionage 101, URL http://www.sans.org/rr/whitepapers/engineering/512.php, Accessed 12/7/2005

Rues, R. (2003) Corporate Open Source Information Leakage, *In Infocon magazine, Issue 1*, URL http://www.iwar.org.uk/infocon/, Accessed 12/7/2005

Schwartau, W. (1996) Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age, Thunders Mouth

Simovits, M. and Forsberg, T. (1997) Business Intelligence and Information Warfare on the Internet, *In International Congress on Information Systems and Telecommunications Security CNIT Paris*, URL http://www.simovits.com/, accessed 12/7/2005
U.S.A.F (1998) Information Operations: Air Force Doctrine Document 2-5, URL http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5.pdf, Accessed 5/4/2005

Waltz, E. (1998) Information Warfare: Principles and Operations, Artech House

Webster, F. (Ed.) (1995) Theories of the Information Society, Routledge

Winkler, I. Case Study of Industrial Espionage Through Social Engineering, URL http://www.simovits.com/archive.html, Accessed 5/4/2005

COPYRIGHT