Information Warfare: Using the Viable System Model as a framework to attack organisations

Bill Hutchinson
School of Management Information Systems
Edith Cowan University
Western Australia, 6018
Tel: +61 (0)8 9273 8283, Fax: +61 (0)8 9273 8332
Email: w.hutchinson@cowan.edu.au

Mat Warren
School of Computing and Mathematics
Deakin University
Geelong
Victoria
Australia 3217
Tel: +61 (0)3 5227 2536, Fax: +61 (0)3 5227 2028
Email: m.warren@deakin.edu.au

Abstract
Information is the glue in any organization. It is needed for policy, decision-making, control, and co-ordination. If an organisation's information systems are disrupted or destroyed, then damage to the whole inevitably follows. This paper uses a proven systemic, analytic framework the Viable System Model (VSM) – in a functionalist mode, to analyse the vulnerabilities of an organisation's information resources to this form of aggression. It examines the tactics available, and where they can be used to effectively attack an organisation.

Introduction

The concept of Information Warfare (IW), which until recently was restricted to military circles, has entered the civilian world. In this information age, with its dependence information and its associated technology, the phenomenon of IW has taken on added significance. In 1993, the increasing importance of IW led the National Defence University in the USA to set up the School of Information Warfare and Strategy (Schwartau, 1996, p.8). According to the US Department of Defence (1996) over 120 countries are developing IW techniques. In the contemporary world, the commercial, social, governmental, and military infrastructures are tightly intertwined. Commercial and government organisations are vulnerable to this type of attack, and some already have been affected by it. For example, in November 1998 (Barton, 1998), it was reported that a hacker wiped out more than 4500 New Zealand web sites. Cobb (1998, p.26) cites an Australian bank's compliance and fraud officer, who admits that the cost of information attack to be in excess of $500 000. Denning (1999) cites many more examples of larger impacts on organisations, and the potentially disastrous effects on the social fabric and economy they can pose. It is an issue of concern for both large and small organisational systems.

This paper outlines possible modes of information attack using the Viable System Model as a framework. It is an attempt to use a systemic tool to expose vulnerability of the information infrastructure in all organisations. Its emphasis is on the attack process, not on counter-attack, counter-measures, or detection. These latter two elements are the province of the security function. Of course, knowledge of attack strategies inevitably increases the effectiveness of counter-measures.

Information Warfare (IW)

IW is the use of information, or information systems to disrupt or destroy an organisation perceived to be an 'enemy'[1]. The over-riding objective being to coerce the target to act in a way that is favourable to the attacker[2]. The use of information to gain advantage over an adversary is not new. However, the magnitude of the impact of these tactics has increased in this information age. Society as a whole is feeling the impact and accompanying massive changes as information increasingly becomes a source of power, influence, and economic gain.

This paper will examine what Schwartau (1996) calls 'Class 2: Corporate Information Warfare'. It includes areas such as industrial espionage, knowledge theft, as well as the more conventional competitive practices of organisations. Firstly, possible tactics for information warfare will be discussed. Secondly, a brief description of the Viable System Model (VSM) will be given to illustrate the functions of a viable organisation espoused by this model. Finally, the tactics and the VSM will be brought together to illustrate possible attack strategies using the VSM as a framework.

Tactics

There are a number of ways information, or information systems can be used to gain advantage over (or disadvantage) another organisation. Some aggressive tactics (developed by the author) are listed below:

- Information can be manipulated, or 'created' (disinformation) to provide the target or its environment (for example, clients) a perception that develops behaviours detrimental to the target, or beneficial to the attacker. At one level, this can be viewed as advertising, and at another, deliberate deception.
- Information can be intercepted, thus giving the interceptor an advantageous insight into the target's strengths, weaknesses, and intentions. This information can be gained legitimately, or illegitimately.
- Information flows in the target organisation can be disrupted, or stopped, thereby interfering with the normal processes of the target producing an advantage for the attacker.
- A target organisation can be 'flooded' with information, thereby slowing or stopping effective processing or analysis of the incoming information.
- Information can be made unavailable to a target organisation by destroying the storage medium, or cutting off the information source.
- Disrupting their availability, or making them produce incorrect/dubious output can lower the credibility of information systems.
- Confidential or sensitive information can be exposed to the public, clients, government agencies, and so on, thereby embarrassing or in other ways harming the organisation.

Knecht (1996, p.168) describes means of attack with a more military emphasis. These are listed below:

- Physical attacks on the components of the information infrastructure.
- Physical attacks on the components containing the information infrastructure.
- Physical attacks on or the subversion of the people (witting or unwitting) who operate elements of the information infrastructure.
- Physical destruction of information (erasure or overwrite) without harming the infrastructure components.
- Logic (malicious code) attacks on the components of the information infrastructure.
- Logic attacks on computer-controlled components supporting the information infrastructure.
- Attacks on the information provided via the information infrastructure to specific functions.
- Corruption of information using logic or digital attacks without harming the components of the information infrastructure.
- Combined attacks on the information infrastructure or supporting components to mask other types of attacks, or to obtain the benefits of a combined attack.

Obviously, many of these tactics are not pertinent to the contemporary business world (at least, not any ethically based corporate strategy) but they do give an idea of the range of possibilities open to an attacker.

The form of attack can be varied. It depends on such factors as the medium of information transfer and storage (for example, electronic, telephone, verbal, facsimile, etc.), the legality of the attack, and the technology used (for example, electronic surveillance, computer viruses[3], and human senses). Rathmell et al (1997) give a number of likely means for penetrative attacks which can be found in Table 1. Other more physical means, such as Directed Energy Weapons, can be used to destroy hardware (Waltz, 1998).

ATTACK TACTIC	COMMENTS
Compromised trusted user	Most software attacks and computer crimes are carried out by trusted users.
Acquisition of user's password	Can be achieved by packet sniffers, and password crackers.
Trojan Horses	Installed after penetration. Mimic actions of system utilities. Useful for sabotage, extortion, and blackmail.
Software Bombs	Similar to Trojan Horses. Planted with some mission critical software, and triggered by date/time.
Viruses	Many variations. Almost all computer systems have been infected at some time.
Worms	Replicate themselves and consume system and network resources.

Table 1: Methods of attacking a computer system/network (Summarised from Rathmell et al, 1997)

Motivations for attacks can have an organisational purpose, or be purely malicious. Attacks can be by individuals or groups. Attackers can be internal to the organisation, or come from individuals or groups external to it. Not all the information involved needs to be confidential, much of it can be in the public domain. Rathmell et al (1997) posit the three main reasons for terrorist groups to use information warfare as raising funds, propaganda campaigns (mostly through Web sites), and to attack the organisation's information infrastructure.

Denning (1999) lists five classes of resources involved in information warfare. They are:

- containers, eg computer and human memories
- transporters, eg humans, telecommunication systems
- sensors, eg scanners, cameras, microphones, human senses
- recorders, eg disk writers, printers, human processes
- processors, eg microprocessors, humans, software

Each of these elements, or groupings of them, can be the foci of attacks. Thus, the range of targets can vary from public opinion to a microwave link.

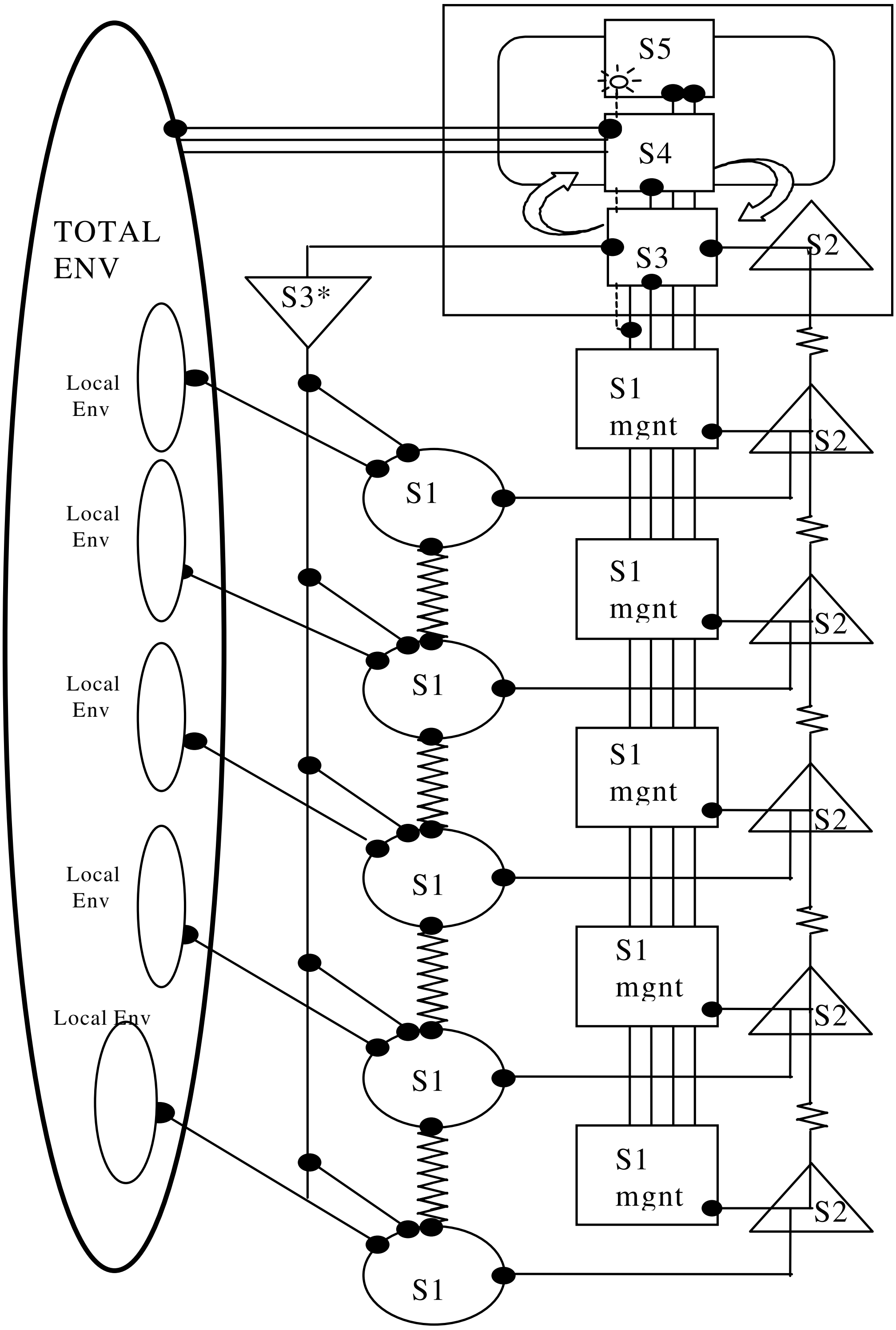
Each combination of attack factors for example, information and communication medium, type of attacker, tactic, and determination of attacker (opportunistic/long term) make protection against every factor difficult. The points of vulnerability in an organisation will now be examined using the Viable System Model (VSM) and its associated functions as a framework for attack.

The Viable System Model (VSM)

The Viable System Model (VSM) developed by Stafford Beer (1985), using the principles of cybernetics has been successfully used to diagnose existing organisational structures and design new ones. As Espejo (1993, p. 522) states *"VSM provides a language in which to appreciate the complexity of organisational tasks and the communication mechanisms underlying people's interactions"*. It is the generic nature of the VSM that allows it to be used in a myriad of circumstances for organisational analysis. It is a metaphor for a robust organisation (system), and can be used to analyse organisational health, and other systemic problems. However, its insights into the requirements of maintaining a viable organisation can also provide clues to the mechanisms for destroying the same. This paper will use this model as a framework to analyse potential vulnerabilities to an organisation's information systems. Its ability to be used in this manner demonstrates VSM's insights into the requirements of a functioning system.

Before using the VSM, it is essential to understand the dynamics of its applicability and a diagrammatic representation is shown at Figure 1. The VSM consists of five subsystems, which have the following functions:

1. **Implementation** (S1): this function consists of semi-autonomous units, which carry out the operational tasks in the system. These are the functions that are basic to the existence/purpose(s) of the system. They interact with their local environment, and each other. Each unit has its own local management, which is connected to wider management by vertical information flows. This function is the 'doing' part of an organization. The VSM has a recursive element, and each S1 has another VSM embedded in it.



(Note: Env = Environment, mgnt = management)

Figure 1: The Viable System Model (after Beer, 1985)

2. **Co-ordination** (S2): this function co-ordinates the S1 units to ensure that each S1 unit acts in the best interest of the whole system, rather than its own. This could be represented by something as simple as a timetable, or as subtle as morale among the workforce.
3. **Internal Control** (S3): this function interprets policy information from 'higher' functions (S4), and 'lower' functions. It is the function, which controls the operational levels. Its function is not to create policy, but to implement it.
   Information arriving from the S1 function must periodically be audited for its quality and correctness. This is the S3* audit function.
4. **Intelligence and Development** (S4): this function acts as a filter of information from the S3 function and the overall outside environment. Its purpose is to ensure that the policy making function (S5) is adequately briefed, and decisions are transmitted to S3.
5. **Strategy and Policy** (S5): this function is responsible for the direction of the whole system. It must balance internal and external factors.

Beer (*ibid.*) contends that all the above functions must be adequately performed in an organisation to keep it viable. It should again be noted that the model has a recursive element. Each S1 unit has embedded in it, another VSM. Hence, the local environment now becomes the total environment for that system, and so on. More detailed descriptions of the VSM can be found in Beer (1984, 1985), Jackson (1991), and Flood and Jackson (1991).

The VSM concentrates on functions but provides an effective tool for specifying information flows throughout the organisation. It explicitly states what needs to 'go on' in a healthy system, and hence the information channels needed to ensure it. It illustrates the need for both internal information for stability, and external information for survival in its environment. The comprehensive nature of the model enables it to be used to design information system strategies, and examine any missing components. Obviously, these qualities can be used to build and expose weaknesses in existing systems. However, these same characteristics can be used to attack organisations, and exploit weaknesses.

Attacking the organization

A planned attack can be made at the operational, tactical, or strategic level. Roughly, these three levels can be mapped against the S1, S2/S3, and S4/S5 functions of the VSM respectively. Also, they can be equated with the efficiency, effectiveness, and vision/purpose of the organisation. Another perspective can be based on time. In this case, the objectives may be short, medium, or long term. In a world of a ubiquitous mass media, and instant, universal communications "the distinctions between the tactical, operational, and strategic tend to blur into insignificance" (Dearth and Williamson, 1996, p. 25). For example, a campaign of misinformation claiming food poisoning caused by a particular product picked up by the mass media can change a local affair to a strategic one as the producer's total environment becomes involved.

Each specific function will now be examined. However, the recursive nature of the VSM, with each S1 having VSM embedded in it, should be noted.

Attacking the fundamental operating units (S1)

The operating units can be disrupted by:

- denying them their operating (local) environments,

- disconnecting them from other S1 units,
- separating them from the management functions.

Information can be used to misinform both the local environment and the S1 units. This can cause a decrease in the beneficial relationship between the two. Disrupting the relationships between S1 units can result in the fragmentation of the whole operations function. This can be achieved by giving different information to each S1 either internally, or from the environment. This will cause a misreading by S1 management units of both their own local environments, and the performance of other S1 units. Attacks on the information flows from S2 and S3 can lower the effectiveness of S1 management.

Attacks on the S1 units are intended to decrease the efficiency of the whole organisation by disrupting its operational (production) functions. It can be viewed as analogous to the classic, military aim of 'breaking the line'. Here the attacker's objective is to disperse the enemy by such things a concentrated attack on a specific part of the line, or striking at its flanks. In information warfare terms, this means using information tactics to cause chaos to a specified S1 unit (a direct attack), or disrupting the information between S1s and/or higher S2/S3 functions (a flanking move).

Attacking the coordinating function (S2)

The purpose of attacking the co-ordinating function (S2) is to destroy the cohesion of the operating units. Such simple things as a timetable, production schedule, or more abstract entities such as staff morale can bring about cohesion. Therefore, the aim of the attacker is to manipulate, change, or deny information to make this co-ordinating function ineffective. Thus, the activities of S1 units would be uncoordinated at the very least, and working against one another to the point of complete disruption in a highly successful attack. An example might be to spread misinformation designed to create negative perceptions amongst staff thereby causing a loss of morale.

The coordinating function can be disrupted by direct attacks on communication or information systems causing the malfunction, or more indirectly by subtlety changing pertinent information causing the integrated functions of the S1 units to fail. Classic psychological operations can be used against the victim's staff (as it can be in the local S1 environment, and more general organisational environment to change perceptions of customers, suppliers, authorities, and the public).

Attacking the controlling function (S3)

The main point of attacking the control function is to use information to disrupt the interpretation of policy. Thus, the instructions passed down to the S1 units would not be commensurate with the intentions of the policies created by S5. Altering information coming into S3 from S1 and S3*, and leaving S3 for S4 will also disrupt or misinform S4. Hence, the formulation of policy will be corrupted by 'bad' information, or be less effective because of lack of information.

Attacking the S3 function should disrupt or destroy effective co-operation between the planning/policy aspects of the organisation and its operating functions. The main intention is therefore is make the operational units either non-functional, or to function in a way that is at odds with the policy making function, and to the benefit of the attacker. Therefore the destruction, or probably more effectively, the corruption of information going in and out of the S3 function is the attacker's aim.

Destroying the 'brains' and 'senses' of an organisation (S4/S5)

The purpose of the S4 level is to be the interface between the external and internal environments by processing and communicating information to S5 and S3. S5 produces policy from the information sent by S4. These two functions can therefore be seen as the 'brains' and 'senses' of the organisation. Therefore, the purpose of an information attack at this level is to create false perceptions of both the internal organisational position, and the external environment. Thus, the aim is to create policies and strategies that are inappropriate for the organisation. The ultimate aim is the organisation's demise.

As well as falsifying, or depriving information, emergency (algedonic) signals can be withheld, delayed, or made to occur erroneously (or very frequently) so they will be ignored in the future. S4 could also be 'flooded' with, or fed erroneous information so causing confusion and mistrust of its validity.

According to Richelson (1993, p.3), the main tasks of an intelligence systems (S4) is to collect, process, analyse and produce, and disseminate information. Waltz (1998, p.51) elaborates on this and classifies the levels of 'information' as:

- Data (measurements and observations)
- Information (data placed into context, indexed, and organised)
- Knowledge (information understood and explained)
- Wisdom (knowledge effectively applied)

Therefore, the task of the attacker is to disrupt, deny, or manipulate data to provide the target with no information, or misinformation. If the target obtains data then the attacker's function is to provide misinformation to manipulate the context. For example, to imply that the data is incorrect (or, in fact, to imply incorrect information is correct). At the knowledge level, the attacker could provide further misinformation to interfere with the deductive and inductive processes needed understand information. A classic example of this can be illustrated by the programme of deception executed by the British before the D-Day landings in Normandy in 1944 (Cave Brown, 1975). At later stages, the attacker needs to deny the effective application of the target's knowledge (or, encourage detrimental applications).

Conclusion

This brief outline using the VSM[4] has illustrated the vulnerability of organisations to attack using information, or its associated systems of storage and transmission. Whilst the security function within an organisation has the responsibility to combat such attacks, an effective defence must entail continual monitoring and intelligence to ensure a dynamic response. Information systems tend to be viewed as synonymous with computer systems, yet information is received, stored, analysed, and acted upon in many forms within an organisation. Therefore, information attacks can occur on many elements in organisational systems. This paper has given a framework for an attacker, and thus has also provided a framework for a defence system.

Organisations can be vulnerable at many levels, and organised attacks can have different objectives. An overall attack strategy should attempt to disrupt, manipulate, deny, and destroy information resources at all functional levels of an organisation. Obviously, a robust system would not be a passive victim in this process, but knowledge of possible aggressive tactics will give the victim added abilities to counteract them. Thus the VSM no only gives a framework for attack and but one for defence as well.

References

Anonymous. (1998). *Maximum Security – second edition*, Sams Publishing, Indianapolis.

Barton, C. (1998). Computer Hacker Destroys 4500 Web Sites. In: *New Zealand Herald*, 19 Nov, 1998.

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.

Cave Brown, A. (1975). *Bodyguard of Lies*. Harper and Row, New York.

Cobb, A. (1998). *Thinking About the Unthinkable: Australian Vulnerabilities to a High-Tech Risks*. Research paper 18 1997-98. Department of Australian Parliamentary Library, Canberra.

Dearth, D.H., Williamson, C.A.. (1996). Information Age/Information War. In: Campen, A.D., Dearth, D.H., Thomas Goodden, R (eds). *Cyberwar: Security, Strategy, and Conflict in the Information Age*, AFCEA International Press, Fairfax. pp.13-29.

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

Department of Defence. (1996). *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. (Testimony, 05/22/96, GAO/T-AIMD-96-92).

Espejo, R. (1993). Domains of interaction between a social system and its environment, *Systems Practice*, **6**,5.

Flood, R.L., Jackson, M.C. (1991) *Creative Problem Solving: Total Systems Intervention*. Wiley, Chichester.

Jackson, M.C. (1991). *Systems Methodology for the Management Sciences*. Plenum Press, New York.

Knecht, R.J. (1996) Thoughts About Information Warfare. In Campen, A.D., Dearth, D.H., Goodden, R.T. (eds). : *Cyberwar: Security, Strategy, and Conflict in the Information Age*, AFCEA International Press, Fairfax. pp. 161-174.

Kuehl, D.T. (1996). Strategic Information Warfare and Comprehensive Situational Awareness. In: Campen, A.D., Dearth, D.H., Goodden, R.T. (eds). *Cyberwar: Security, Strategy, and Conflict in the Information Age*, AFCEA International Press, Fairfax. pp. 185-195.

Rathmell, A., Overill, R., Valeri, L., Gearson, J. (1997). The IW Threat from Sub-State Groups: an Interdisciplinary Approach, presented at *Third International Symposium on Command and Control Research and Technology*, June 17-20, 1997. (Available on-line at: http://www.kcl.ac.uk/orgs/icsa).

Richelson, J.T. (1995). *The U.S. Intelligence Community – third edition*. Westview Press, Boulder.

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

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

[1] There are numerous other definitions of IW. For example, Knecht (1996, p. 165) offers "The preparation for and use of physical or logic-based weapons to disrupt or destroy information or

information systems in order to degrade or disrupt a function(s) that depend upon the information or information systems".

[2] The conventional information systems (IS) function is to exploit information for the organisation's benefit, whilst the security function should protect it. The information warfare function is to deny, disrupt, or destroy a target's IS function. Waltz (1998), although concentrating mostly on military and national IW, gives a good background to the topic.

[3] There are many good texts on computer attack methods such as spoofing, worms, viruses, and spamming. A recent comprehensive publication can be found in the References section (Anon, 1998).

[4] Of course, there are many organisational models that could be used. For instance, Warden's concept of Rings and Systems (cited in Kuehl, 1996, pp.187-189) can be used. Here the target is modelled in a series of concentric rings. Each represents (from the outer to inner ring):The fighting mechanism (for example IS security staff), the population (for example, the general staff), the infrastructure (for example, power, communication systems, and networks), the organic essential (for example, money, and production inputs), and leadership. Each attack can be aimed at any of these rings. Classic theory would have the inner 'leadership' ring as the target, which would be a 'war winner'.