

The George Washington University

Applying Information Warfare Theory to Corporate Strategy

EMSE 318.10 – Information Operations

Fall 2002

Dr. Julie JCH Ryan

School of Engineering Management and Systems Engineering

By

Andrew J. Downey

Annandale, VA

December 4, 2002

Certification of Authorship

This paper is my own work. Any assistance I received in its preparation is acknowledged in this paper, in accordance with standard academic practice. If I used data, ideas, or words from any source, I have cited the sources fully and completely. This includes sources from which I have quoted or paraphrased. Furthermore, I certify that this paper was prepared by me for this class specifically.

Signed: \_\_\_\_\_ Date: \_\_\_\_\_

## Contents

	page
Table of Contents	ii
Abstract	iii
Tables	iv
Figures	v
Introduction	1
Information Warfare Defined	2
Information Warfare Models – Waltz and Denning	5
<i>The Waltz Model</i>	5
<i>The Denning Model</i>	7
Business Strategy in a Global Context	10
Information Warfare Tactics in the Corporate Context	13
Business Strategy and SWOT analysis	16
A New Approach to Corporate Strategy: IW-SWOT analysis	19
<i>Layer 1 – perceptual</i>	20
<i>Layer 2 – infrastructure</i>	21
<i>Layer 3 – physical</i>	22
Applying the IW-SWOT analysis	23
<i>Entering a Foreign Market</i>	23
<i>IW-SWOT in the context of a hostile takeover</i>	25
The Decision Making Process and the OODA Loop	27
Conclusion	32
Bibliography	34
<i>Books</i>	34
<i>Journal Articles</i>	37
<i>News Articles</i>	40

## Abstract

Information warfare theory is applied corporate strategy in both operational and strategic frameworks. Such an application is appropriate for two reasons. First of all, the changing nature of international relations between nation-states, international corporations and non-governmental organizations from a cold-war, competitive mindset to one based on cooperation in the new world order. This change from realpolitik to 'noopolitik' has tremendous repercussions for international security, law enforcement, and commerce based on intellectual property. Second, is the increased reliance upon informational infrastructures as the means of production and communication.

Two models of information warfare are presented. The Waltz model is described and integrated with traditional SWOT analysis to present a way of formulating corporate strategy, or as a method of estimating the risks associated with particular strategies. The IW-SWOT model described here can be used to develop strategy or as a way to re-allocate resources to deal with changes in the threat matrix posed by competitors, governments and other organizations. Examples of information warfare tactics are discussed and the IW-SWOT model is applied to hypothetical situations.

The Denning model of information warfare is also examined and applied to the strategic decision making process, as illustrated by the OODA loop. Due to its zero-sum nature, the Denning model is more appropriate than the Waltz model for examining the information warfare tactics and strategies that businesses may employ against one another. Corporate competitive intelligence and counter-intelligence/espionage programs are described as tactics for which the Denning model can be used.

## Tables

Table	page
Table 1 – Characteristics of the Operational Model of Information Operations	6

## Figures

Figure	page
Figure 1 – Risk Management Model	7
Figure 2 – Denning Information Warfare Model	8
Figure 3 – SWOT Analysis	17
Figure 4 – IW-SWOT analysis	20
Figure 5 – OODA Loop	28

## Introduction

The term “military-industrial complex” is suggestive of a symbiotic relationship between the military and corporate worlds. Indeed, most of the equipment and supplies used by the American Armed Forces is produced by private-sector firms, both foreign and domestic. In addition, many of the domestic firms who supply the American military also sell their products overseas.

Similarly, new technologies flow both ways. The Global Positioning System (GPS) was originally developed for military use, but now many commercial firms use the technology for guidance or to monitor their assets.<sup>1</sup> The Internet is another technology that has grown from its military roots into a powerful tool for business. Conversely, military planners are adopting corporate communication models – such as those used by Wal-Mart – to help fight the war on terror.<sup>2</sup> This symbiotic relationship will continue to grow stronger in the future as warfare becomes more dependent upon the critical infrastructure owned and operated by private firms. As such, it seems likely that the two worlds will continue to influence each other to a greater extent.

This paper examines Information Warfare theory and applies some of the concepts in a corporate context. Can information warfare theory and information warfare models be used to help shape corporate strategy? If so, how? Contemporary examples of corporations using or being accused of information warfare-like tactics can be found in

---

<sup>1</sup> Robert Lemos, “Rental-car firm exceeding the privacy limit?” *Tech News – Cnet.com*. June 20, 2001. [Internet] at <http://news.com.com/2100-1040-268747.html?legacy=cnet> .

<sup>2</sup> Thomas A. Stewart, “America’s Secret Weapon” *Business 2.0*, December 2001, pp. 58-68.

the news.<sup>3</sup> Competitive intelligence is a growing discipline and concern over corporate espionage is not new.<sup>4</sup> Two models of information warfare are discussed and applied to contemporary business strategy – both business operations and the business decision making process.

### Information Warfare Defined

Information warfare has become somewhat of a marketing buzzword, and this has led to a dilution of its true meaning. There are many definitions, usually colored by the goals or mission of the group or organization defining the term.<sup>5</sup> However, for purposes of this paper, information warfare will be defined as:

Information warfare is, first and foremost, warfare. It is not information terrorism, computer crime, hacking or commercial or state-sponsored espionage using networks for access to desirable information.... InfoWar is the application of destructive force on a large scale against information assets and systems, against the computers and networks which support the air traffic control systems, stock transactions, financial records, currency records, Internet communications, telephone switching, credit records, credit card transactions, the space program, the railroad system, the hospital systems that monitor patients and dispense drugs, manufacturing process control systems, newspapers and publishing, the insurance industry, power distribution and utilities, all of which rely heavily on computers.<sup>6</sup>

Information warfare is practiced on many levels. The first level is the physical infrastructure – such as the power grid and telecommunication lines and facilities – that

---

<sup>3</sup> Rachel Ross, “DirectTV Move KOS Bootleg Access Cards,” *The Toronto Star*. January 30, 2001. See also Lauren Chambliss, “Hiring ‘Big Gun’ hacker backfires on Murdoch.” *The Evening Standard (London)*. October 10, 2002. p. 41.

<sup>4</sup> Dorothy E Denning, *Information Warfare and Security*, New York: Addison Wesley, p. 146. Denning gives an account of nineteenth century espionage concerning textile manufacturing secrets. For the purposes of this paper, competitive intelligence and corporate espionage are defined as different sides of the same coin. Both try to discern the business plans and trade secrets of competitors; however, competitive intelligence uses legal methods, such as open source data collection, whereas corporate espionage has no regard for ethics or law.

<sup>5</sup> See Gregory J.Rattray, *Strategic Warfare in Cyberspace*. Cambridge: MIT Press. pp. 1-21., for a number of information warfare definitions.

<sup>6</sup> Daniel J. and Julie JCH Ryan , “Protecting the National Information Infrastructure Against Infowar,” in Schwartau, *Information Warfare*, 627., cited in Rattray, p.12.

can be targeted by kinetic weaponry. One of the first targets destroyed in Operation Desert Storm was the main telephone center in Baghdad, leading to a communications crisis among the Iraqi command and control system.<sup>7</sup>

Moving up from this level is the network itself: switches, hubs, and routers. These devices can be targeted for disruption or flooded with traffic leading to denial-of-service conditions.

Next, are the operating systems of the computers connected to the network. Many different types of attacks exist here. These attacks may be used by attackers to gain unauthorized access to computers or cause them to crash. Sometimes these attacks are coded into self-replicating programs called *worms*. These worms often flood networks with traffic, resulting in a denial-of-service condition.

Programs that run on these operating systems can also be attacked. An attacker may insert code that causes a program to crash or operate in a manner not intended by the original programmer.

Finally, there is the data that these programs process, store, and transmit. Data can be destroyed or altered; both techniques render the information useless to its owners. However, alteration may be more damaging because unless it is detected, the altered data may still be relied upon as if it were still valid. This has two negative effects; (1) resources are used to maintain this corrupt data; and, (2) as the data is integrated into other parts of organization – for example, in the use of simulations or models – the corruption spreads like an infection.

---

<sup>7</sup> Denning, p. 5.

But information warfare does not stop here. How people interpret the information they are presented with is also another area where information warfare techniques are used. Deception can be used to cause an enemy to defend against nonexistent threats, . Examples of this include the fake army – including inflatable rubber battle tanks – the allies built in WW II to convince the Germans that Normandy was not the intended D-Day invasion point. Even after the invasion began, the Germans were still convinced the invasion was going to be further up the French coastline. During Desert Storm, U.S. Forces staged amphibious assaults to trick the Iraqi forces into thinking that an amphibious assault would be used to flank the Iraqi forces in Kuwait.<sup>8</sup> After the war began, a SEAL team infiltrated into the beach and set off explosive charges, causing Iraqi armored units to redeploy to fend off an amphibious assault that never came. These examples follow the tenet that it is easier to deceive people into following their preconceived notions than it is to convince them that their perceptions are wrong.<sup>9</sup>

Information warfare also seeks to leverage its effects. First, information warriors identify centers of gravity – those informational infrastructures upon which nation-states, corporations, and other organizations are dependent – and target these centers for disruption.<sup>10</sup> Usually, attacks on these centers of gravity will produce cascading effects:

The ‘cascade’ concept refers to the effect of a particular system failure resulting in the promulgation of a much broader set of disruptive effects. A widely cited example is the power outage in the northwest United States in August 1996 resulting from automated shutdown procedures that began when a tree growing into a power line caused a local power system problem.<sup>11</sup>

---

<sup>8</sup> Ibid, p.6.

<sup>9</sup> Richards J. Heuer, Jr., “Strategic Deception and Counterdeception: A Cognitive Systems Approach.” *International Studies Quarterly*. Volume 25, Issue 2, June 1981. pp. 294-327.

<sup>10</sup> Rattray, p. 27.

<sup>11</sup> Ibid., p. 132.

Despite its original design of redundancy, the Internet is susceptible to similar cascading effects. In July 2001, a train caught fire in a Baltimore tunnel and damaged a fiber-optic cable. The result was widespread, including cell phone disruption in Maryland and e-mail outages in Africa.<sup>12</sup>

### Information Warfare Models – Waltz and Denning

#### *The Waltz Model*

Edward Waltz provides a thorough and complex discussion of information warfare in his book, *Information Warfare Principles and Operations* (Artech House, 1998). His framework describing an operational model for information operations is described in detail in chapter five in his book. A summary is found in table 1.

According to Waltz, information warfare must consider each level of the model. For example, consider his description of how intelligence gathering must take into account all three layers:

Layer 1 – Intelligence should include an estimate of the target’s current perception, uncertainties, concerns, critical decisions, decision-making processes and authorities, and decision time lines. The perceived courses of action available to the target, and the decision constraints, should be understood.

Layer 2 – Intelligence must describe the information infrastructure: information structures, protocols, communication and computing network structures, switching and fusion nodes, decision points, power grids, security characteristics, and so forth, with an assessment of vulnerabilities.

Layer 3 – Finally, intelligence must detail the physical characteristics of systems, computers, telecommunications, power, facilities, personnel, and security support barriers to the targeted physical systems.<sup>13</sup>

---

<sup>12</sup> Michaela Cavallaro, “Tunnel Burns, Internet Melts,” *The Industry Standard*, July 20, 2001. Available at <http://www.thestandard.com/article/0,1902,28110,00.html>, accessed June 29, 2002.

<sup>13</sup> *Ibid.*, p. 152.

Table 1 – Characteristics of the Operational Model of Information Operations<sup>14</sup>

<b>Model Layer</b>	<b>Characteristics and Components</b>	<b>Attacker's Operations</b>	<b>Defender's Operations</b>	<b>Desired Effects</b>
<b>Layer 1 Perceptual (knowledge)</b>	Knowledge and understanding in human decision space: <ul style="list-style-type: none"> <li>• Perceptions</li> <li>• Beliefs</li> <li>• Reasoning</li> </ul>	PSYOPS  Diplomacy  Civil and public affairs	Psychological security  Objective aids	Cognitive – influence decisions and behavior
<b>Layer 2 Infrastructure (information)</b>	Information Maintained in Cyberspace: <ul style="list-style-type: none"> <li>• Data structures</li> <li>• Processes</li> <li>• Protocols</li> <li>• Data content</li> </ul>	Network attack, support measures  Electrical power attack	INFOSEC  Information security	Functional – influence the effectiveness and performance of information functions supporting perception and controlling physical processes
<b>Layer 3 Physical (data in physical form)</b>	Data managed in physical space: <ul style="list-style-type: none"> <li>• Computers</li> <li>• Storage</li> <li>• Networks</li> <li>• Electrical power</li> </ul>	Physical electronic attack  Intrusion  Theft  Wiretapping  Destruction	OPSEC  Physical security	Technical – affect the technical performance and capacity of physical systems

This framework provides a powerful way to approach other elements of information security and information warfare, especially when combined with the information security risk management model presented by Nichols et al, see figure 1. The level of risk that an organization is a function of the particular threats and vulnerabilities the organization faces, the countermeasures deployed against these threats and vulnerabilities, as well as the impacts of a successful attack.

<sup>14</sup> Edward Waltz, *Information Warfare Principles and Operations*, Boston: Artech House. p. 151.

Figure 1 – Risk Management Model<sup>15</sup>

$$\text{Level of Risk} = \frac{(\text{Threat} \times \text{Vulnerability})}{\text{Countermeasures}} \times \text{Impact}$$

At each layer, the corporation must ask, what are the threats? Where are the corporation's vulnerabilities? What kinds of countermeasures are available? How significant are the impacts? These questions should be asked for both effects on personnel and information technology. Further analysis should look at questions such as: Are there centers of gravity at any of these layers? What about the possibility for cascading effects?

### *The Denning Model*

Dorothy Denning presents a different model of information warfare in her book, *Information Warfare and Security* (Addison-Wesley, 1999). She provides a more simplistic definition of information warfare:

Information warfare consists of offensive and defensive operations against information resources of a "win-lose" nature.<sup>16</sup>

She takes the information security CIA triad – confidentiality, integrity, and availability – and rearranges it so that confidentiality is considered part of information availability (i.e. confidentiality is preventing the information resource from being

---

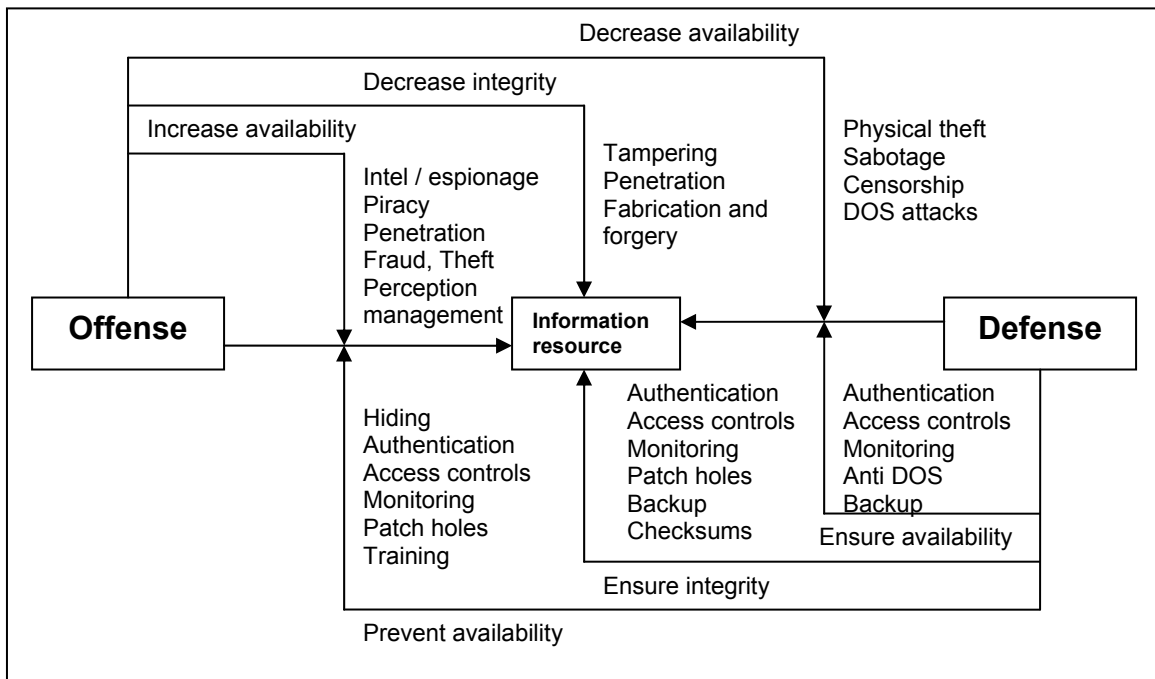
<sup>15</sup> Randall K. Nichols, Daniel J. Ryan, and Julie J.C.H. Ryan. *Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves*. New York: McGraw-Hill. p. 70.

<sup>16</sup> Denning, p. 21.

available). This then sets the stage for the “offense” and “defense” to compete in win-lose, zero-sum-gain struggles along twin axes of availability and integrity, see figure 2.

The offense and defense are engaged in two battles. The first battle is information integrity, as shown by the middle set of arrows in figure 2. The defense will deploy countermeasures such as authentication, access controls, monitoring, patching, backing up data and employing cryptographic checksums to help ensure the integrity of its data and systems (the information resource). Against this, the offense will attempt to violate the information resource’s integrity through the use of tampering, penetration, fabrication and forgery. Any gain by the offense is a loss to the defense, and vice-versa.

Figure 2 – Denning Information Warfare Model<sup>17</sup>



<sup>17</sup> Ibid., p. 31.

The second battle is over the availability of the information resource. Denning's model defines confidentiality as preventing the information resource from being made available to the opposition. This is in addition to the more traditional availability definition – the capability to make use of one's information resources in a timely manner.

For the first instance of availability, the offense will attempt to access the defense's information resources through the use of intelligence (both competitive intelligence and corporate espionage), piracy, penetration (both electronic and through the use of social engineering), fraud, theft, or perception management. The defense will deploy countermeasures against these attempts, such as hiding, authentication, access control, monitoring, applying patches, and training and awareness. Again, this dynamic is of a win-lose nature, one side's gain is the other's loss.

The other availability dynamic uses some of the same tactics, but the goal here for the defense is to ensure that the information resource is available for use. The offense is not trying to access the information resource, but rather, prevent the defense from being able to make use of it. To do so, the offense may use physical theft or destruction, sabotage, censorship or electronic denial-of-service attacks. The defense has a number of tools and techniques at its disposal: authentication, access control, monitoring, anti-denial-of-service infrastructures and backup systems. Again, the struggle between offense and defense is a zero-sum-gain.

Although the Waltz and Denning models appear different, they use many of the same techniques, strategies and tactics. They are both applicable to similar situations, and may produce similar results. However, when applied to business strategy, especially in a global context, one model may be preferable to the other depending upon the course

of action being assessed. The Waltz model is better suited to take into account factors that are not necessarily adversarial – such as regulatory or legal structures – whereas the Denning model and its win-lose construct is better suited to look at competitors and the corporate decision making process.

### Business Strategy in a Global Context

The global geopolitical business environment has changed significantly since the end of the cold war. New political relationships between countries have opened up new markets and new information technologies have brought those foreign markets closer to home. However, this new world presents danger as old players are reorganized into new alliances. There are those who embrace this new world and those who cling on desperately to the old one.<sup>18</sup> Nation states are losing power to international organizations and international businesses. Sometimes this loss of sovereignty leads to disastrous results, giving rise to a sometimes violent anti-globalization movement.<sup>19</sup> The power of the gun is being usurped by the power of culture, ideas and money. We are witnessing a shift away from the realpolitik of the cold war and towards what RAND scholars John Arquilla and David Ronfeldt have termed “noopolitik”:

‘Noopolitik’ as “foreign-policy behavior for the information age that emphasizes the primacy of ideas, values, norms, laws, and ethics – it would work through ‘soft power’ rather than ‘hard power.’<sup>20</sup>

---

<sup>18</sup> Thomas L. Friedman, *The Lexus and the Olive Tree*. New York: Farrar, Strauss and Giroux 1999 pp. 322-329. He describes the rise of the “Super-Empowered Angry Man” and describes the threat that these individuals pose to the western world and America in particular.

<sup>19</sup> Joseph E. Stiglitz, *Globalization and its Discontents*. New York: W.W. Norton & Company 2002. Stiglitz claims IMF policies throughout the 1990s did more harm than good to recipient countries.

<sup>20</sup> John Arquilla and David Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy*, Santa Monica: RAND 1999. p. x.

Noopolitik has political, military, economic and legal implications that we are just beginning to understand. What is obvious, however, is the importance of the global information infrastructure to this new world order.

Common defense, in terms of information strategy, refers to the notion that all members of a security regime or alliance must have similarly strong remedies against threats to their information infrastructures. Because of the deeply interconnected nature of information security, compromise of one sector could have serious effects upon the whole.<sup>21</sup>

This has significant legal and economic implications that will affect international corporations:

From an economic-legal perspective, this cooperation may depend upon reaching agreement in several issue areas, beginning with what might be called “substantive law.” This notion basically calls for agreement as to what constitutes a “crime,” including fraud, forgery, hacking, and sabotage (or as we have called it, “cybotage”).<sup>22</sup>

We may even see a completely separate system of law develop outside of current legal structures.<sup>23</sup> Businesses strategy will need to take into account the legal landscape, not only for what protection it may offer, but for the threats and liabilities that it may pose.

Businesses compete against each other to gain a greater share of markets, which by their nature are finite resources. The simplest strategy is to do one of two things: (1) offer a comparable product or service at a lower cost; or, (2) provide a better good or service for the same price. However, in today’s global marketplace things are much more complicated. Corporations compete against each other in a variety of additional ways.

---

<sup>21</sup> Ibid., p. 59.

<sup>22</sup> Ibid., p. 57

<sup>23</sup> David R. Johnson and David Post, “Law and Borders – the Rise of Law in Cyberspace.” *First Monday*. Volume 1, number 1, May 6, 1996. [Internet] available at <http://www.firstmonday.org/issues/issue1/law/index.html>.

One of these ways is through the use of perception management, defined by Denning as “operations that exploit an information medium available to a target population ... in order to affect their beliefs and ultimately behavior.”<sup>24</sup> In fact, this is one area where the corporate world excels. The Pepsi Challenge launched in 1993 is such an example.<sup>25</sup> Occasionally businesses may target their competition explicitly and hide behind a third party proxy. An example of this tactic is the Web site allegedly sponsored by Proctor & Gamble that encouraged complaints against Amway.<sup>26</sup> Another example is the current “Voices for Choices” campaign in which SBC is targeted and painted as a greedy and unethical corporation. However, looking beyond the television commercial reveals the “voices” behind the campaign belong to some of SBC’s competitors. In fact, the whole campaign is an attempt to influence telecom regulation.<sup>27</sup> Government, and the regulations it promulgates, is often used as a proxy for corporations to try to gain advantages over each other. One high-profile example of this is the U.S. Government’s antitrust suit against Microsoft. This legal battle was started at the behest of a competitor.<sup>28</sup> This trend may only become more common as the lines between government and business, especially in a global context, blur.

---

<sup>24</sup> Denning, p. 34.

<sup>25</sup> Benjamin Gilad, *Business Blindspots 2<sup>nd</sup> Edition*. Wiltshire, England: Infonortics 1996. p.81.

<sup>26</sup> Paul Bocij, “Corporate Cyberstalking: An Invitation to Build Theory.” *First Monday*. Volume 7, number 11, November 2002. [Internet] available at [http://firstmonday.org/issues/issue7\\_11/bocij/index.html](http://firstmonday.org/issues/issue7_11/bocij/index.html).

<sup>27</sup> Judy Newman, “Telecom Companies Use Ad Blitz: SBC Ameritech Isn’t Happy Letting Other Companies Use Its Lines.” *Wisconsin State Journal*. November 1, 2002. p. E1.

<sup>28</sup> Michael Lewis, *The New New Thing: a Silicon Valley Story*. New York: W. W. Norton & Company 2000. pp. 191-194.

Governments are not the only proxies used by businesses as they compete with each other. Special consultants, known as “kites” will be employed to gather information about other companies, often using unethical or illegal methods.<sup>29</sup> Often these kites will use social engineering techniques to elicit information. Corporate espionage is especially harmful if the offense is able to gain inside access, either as a consultant, an employee or a service worker. In one high-profile case, an insider was able to abscond with over a billion dollars worth of information after a day and a half on the job.<sup>30</sup> Hackers are getting in on the action too, breaking into corporate networks on behalf of the competition.<sup>31</sup>

### Information Warfare Tactics in the Corporate Context

These trends suggest that information warfare – also known as “information operations” – may be used by corporations against one another. The use of proxies by corporations is well established. These third parties allow corporations to take actions that the corporation may not be able to do from a public relations or legal standpoint. The next time a corporation finds itself on the receiving end of a “hactivist” group’s DDoS attack, the trail may lead back to its competitors. The use of third parties may not always be the case, however, as there are a number of cases where information warfare

---

<sup>29</sup> Adam L. Penenberg and Marc Barry, *Spo0ked: Espionage in Corporate America*, Cambridge: Perseus Publishing 2000. p. 19.

<sup>30</sup> Ira Winkler, *Corporate Espionage: What it is, Why it’s happening in your company, What you must do about it*. Rocklin, CA Prima Publishing 1997. The ‘thief’ was Winkler himself, who was hired by the company to determine how vulnerable it was to corporate espionage.

<sup>31</sup> See Denning, p. 234.

tactics have been allegedly traced back to competitors. Examples exist of competing ISPs ping-flooding their competitors on more than one occasion.<sup>32</sup>

A high profile example of a corporation deploying information warfare tactics comes from Europe. Canal Plus, a Pay-TV subsidiary of Vivendi Universal alleged that NDS, a smart-card business controlled by News Corporation, devoted money and personnel to crack the security mechanism used by Canal Plus to secure its signal.<sup>33</sup> Canal Plus claimed that the public release of the hack and the subsequent proliferation of counterfeit smart cards had cost the company more than \$1 billion. This loss was a contributing factor in the resignation of Vivendi CEO Jean-Marie Messier.<sup>34</sup> Another interesting fact of the case is that the employee at the center of this controversy was trained by the U.S. Army before becoming a hacker and eventually being hired by NDS to help design their smart card systems. The allegations have been hurtful to News Corporation's reputation, and it has also been subpoenaed by the U.S. Department of Justice in the matter.<sup>35</sup>

But corporations employing information warfare tactics are not always unethical; sometimes it can help protect a company's intellectual property and add to the bottom-line. In January 2001, DirectTV, a satellite TV provider, launched an electronic countermeasure against people pirating the company's satellite service. There had been a thriving black market for modified smart cards that would allow people to access the

---

<sup>32</sup> Ibid., p. 236

<sup>33</sup> James Harding and Raphael Minder, "Rivalry erupts in lawsuit over digital television code." *Financial Times (London)*. March 13, 2002. p. 26.

<sup>34</sup> Lauren Chambliss, "Hiring 'Big Gun' hacker backfires on Murdoch." *The Evening Standard (London)*. October 10, 2002. p. 41.

<sup>35</sup> Ibid.

service without paying for it.<sup>36</sup> The information about how to hack the system had been documented on numerous web sites, and hacked cards were often advertised in newspaper classified ads. DirectTV had been monitoring the situation and its technicians developed a countermeasure. They designed a program that would disable the counterfeit cards and downloaded it onto the pirated cards throughout a series of updates. The final piece of the program was downloaded on Super Bowl Sunday, disabling the counterfeit cards and leaving an estimated 200,000 pirates without access to the big game or any other programming. This approach also worked across legal boundaries, for a number of the pirates were in Canada, where selling the hacked cards was not, at the time, illegal.<sup>37</sup> This is a textbook case of a corporation legitimately using information warfare tactics to protect its assets.<sup>38</sup> However, the pirates have fought back, and the technological tug-of-war continues to this day.<sup>39</sup>

Similar strategies will be employed in the future, especially for the protection of intellectual property. Here, corporations will continue to back legal sanctions such as those set out in the Digital Millennium Copyright Act, but will also increasingly look for technological solutions as well. Microsoft's forthcoming Palladium operating system will incorporate hardware based intellectual property protection mechanisms. Whether or

---

<sup>36</sup> Rachel Ross, "DirectTV Move KOS Bootleg Access Cards," *The Toronto Star*. January 30, 2001.

<sup>37</sup> Andy Jones, Gerald L. Kovacich, and Perry G. Luzwick, *Global Information Warfare: How Businesses, Governments and others Achieve Objectives and Attain Competitive Advantages*. Boca Raton: CRC Press. pp. 379-382.

<sup>38</sup> Ibid.

<sup>39</sup> David Leiberman, "Millions of pirates are plundering satellite TV," *USA Today*, December 2, 2002. p. 1A.

not such tactics will succeed remains to be seen. However, it is obvious that corporations will no longer be able to ignore information warfare tactics in their future business plans.

### Business Strategy and SWOT analysis

Business strategy is a complex science. Business leaders must cope with many different issues – marketing, sales, distribution, manufacturing, labor, purchasing, research and development, finance and control and the firm’s product line are some of the issues that management must align with organizational goals such as profitability, growth, market share, social responsiveness and competitive strategy.<sup>40</sup>

Business management must align the corporation’s strategy to its competitive advantage in the markets where it competes. This is done by matching the company’s internal (S)trengths and (W)eaknesses to the external (O)pportunities and (T)hreats presented in the marketplace. This is known as SWOT analysis (figure 3).<sup>41</sup>

Today, the corporation’s information infrastructure plays an important part of the overall strategy. Information systems management is a field with its own theories, strategies and techniques. With the increasing reliance of corporations on their information infrastructure, those firms able to align their information systems strategy

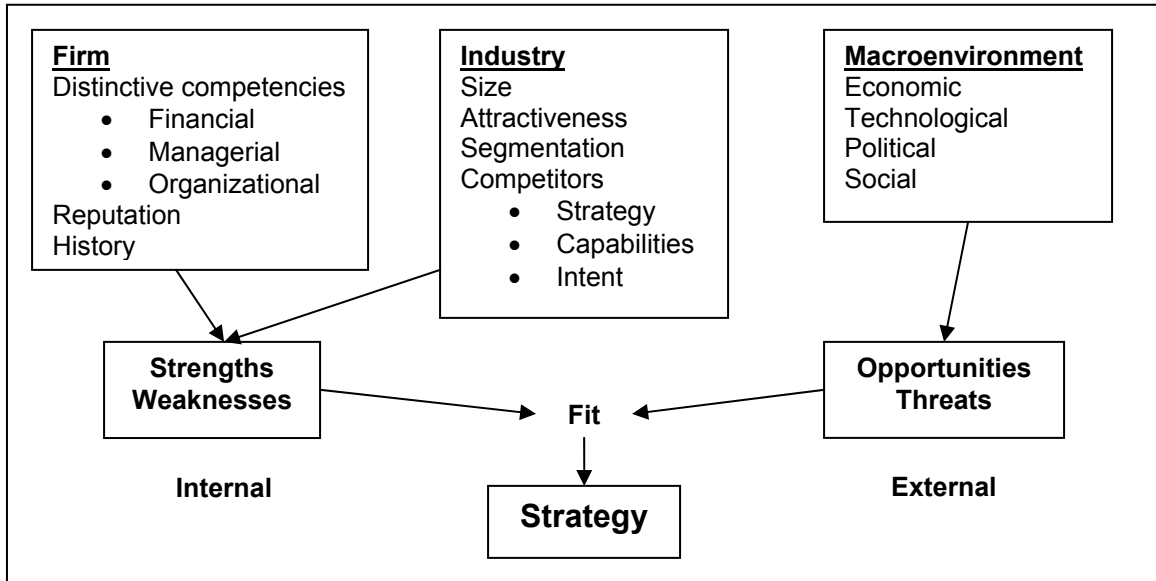
---

<sup>40</sup> Michael E. Porter, *Competitive Strategy*. New York: Free Press 1980, cited in David J. Collins and Cynthia A. Montgomery, *Corporate Strategy: Resources and the Scope of the Firm*. Boston: Irwin 1997. p. 49.

<sup>41</sup> David J. Collins and Cynthia A. Montgomery, *Corporate Strategy: Resources and the Scope of the Firm*. Boston: Irwin 1997. p. 49.

with their larger corporate strategy are more likely to be successful.<sup>42</sup> However, this greater reliance on information infrastructures increases the impacts, and thus the risks

Figure 3 – SWOT Analysis<sup>43</sup>



posed by vulnerabilities in the information infrastructure. For example, corporations are now using databases to profile their customers in order to provide customization previously available only to niche firms.<sup>44</sup> Threats here include changing data held in the database (data diddling), altering the algorithms used to develop customer profiles, or disclosure of these profiles themselves (privacy issues). If the company is heavily dependent upon an online strategy, the fallout from a security breach – such as the

<sup>42</sup> K.M. Delargy, “The New Business Landscape.” *Manufacturing Engineer*. Volume: 80 Issue: 4, Aug. 2001. pp. 169 -174.

<sup>43</sup> Ibid., p.50.

<sup>44</sup> Jim Beeson, “Riding the Marketing Information Wave.” *Harvard Business Review*. September-October 1993. pp. 150-160.

disclosure of a customer's profile – will be even greater because the vendor-customer trust relationship plays a more important role online.<sup>45</sup>

Unfortunately, information security is commonly treated as an afterthought when designing information systems.<sup>46</sup> In fact, IT managers often “expose firms to unfamiliar risks of which they are unaware, refuse to acknowledge, or are often poorly equipped to manage.”<sup>47</sup> Obviously, the solution to this is to hire or train information technology managers so that they understand information security issues and management techniques. Some authors have even described information security in the context of corporate strategy.<sup>48</sup> However, these attempts describe it in a role supporting corporate strategy, a common approach of many firms today. However, in the near future, this approach may not be enough. Brilliant tactics cannot make up for a poor strategy. Thus, to solve the problem presented by corporations' greater reliance on their information infrastructures and to counter information warfare tactics carried out by other

---

<sup>45</sup> Frederick F. Reicheld and Phil Schefter, “E-Loyalty: Your Secret Weapon on the Web.” *Harvard Business Review*. July-August 2000. pp.105-113. It should be noted that this use of the word ‘trust’ in this context refers to the economic context. In information security, the terms ‘trust’ and ‘trust relationship’ have a far more precise and rigorous definition.

<sup>46</sup> Bernard H. Boar, *Practical Steps for Aligning Information Technology with Business Strategies: How to Achieve a Competitive Advantage*, New York: John Wiley & Sons, Inc. 1994. This book covers the history of IT, IT architecture, IT planning and forecasting, the economy. Notably absent is the mention of information security, save for one mention of a need for “security for safeguarding the integrity of information.”

<sup>47</sup> Karen D. Loch, Houston H. Carr, and Merrill E. Warkentin. 1992. “Threats to Information Systems: Today's Reality, Yesterday's Understanding.” *MIS Quarterly*. Volume 16, number 2, June 1992, pp. 173-186.

<sup>48</sup> Blaise Cronin, and Holly Crawford, “Raising the Intelligence Stakes: Corporate Information Warfare and Strategic Surprise.” *Competitive Intelligence Review*. Volume 10, number 3, Q3 1999. pp. 58-65. See also Mary Pat McCarthy, and Stuart Campbell with Rob Brownstein, *Security Transformation: Digital Defense Strategies to Protect Your Company's Reputation and Market Share*. New York: McGraw-Hill 2001.

corporations, hacktivists or governments, it may be beneficial to address these issues at the strategic level.

### A New Approach to Corporate Strategy: IW-SWOT analysis

Applying the SWOT analysis using an information warfare perspective may be beneficial to a corporation, especially those involved with the creation or distribution of intellectual property. Entering foreign markets or competing against companies from abroad may entail a different set of threats, especially if the firm's competitors are from France, Russia or another country whose national intelligence agencies have been known to spy on foreign competitors.<sup>49</sup> This technique may not be a replacement for current business strategy, but may help the firm identify high-risk ventures or to choose between two similar options with different susceptibilities to information warfare tactics. It may also be useful as it considers groups – such as non-state actors – as potential adversaries, a view that may not be explored in other strategic analyses. The Waltz model is better suited for planning business operations strategy, as it can more easily incorporate non-adversarial factors, such as legal structures, into its analysis. The Denning model's win-lose dynamic is less appropriate in this instance, but can be applied in other ways that will be discussed later. The goal of this analysis is to help the firm match its strategy to the situation much as water matches its flow to the earth.<sup>50</sup>

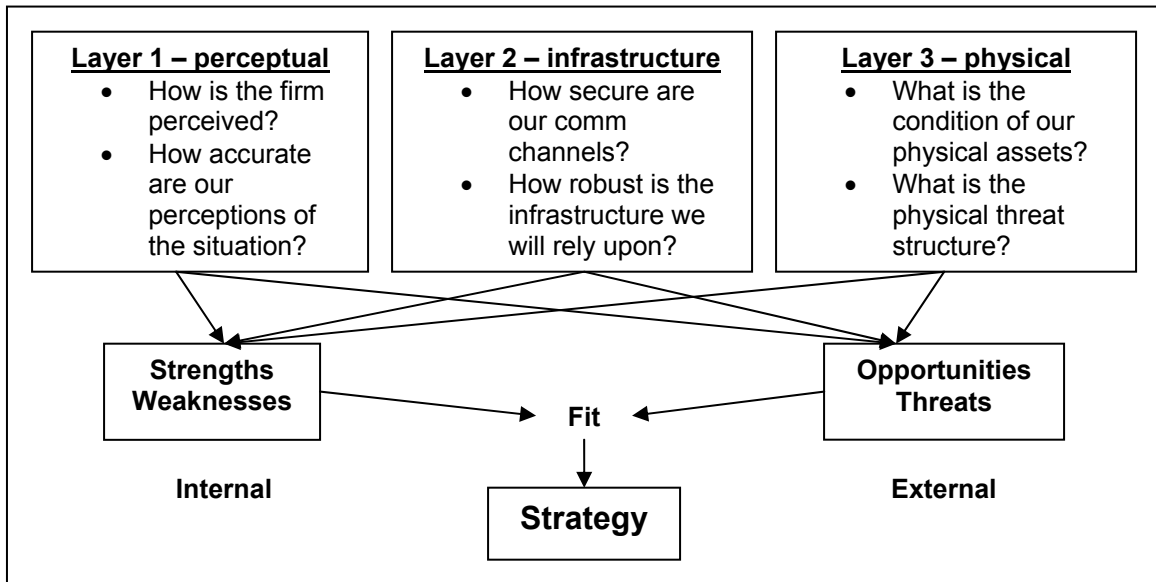
---

<sup>49</sup> Larry Kahaner, *Competitive Intelligence: How to Gather, Analyze, and Use Information to Move Your Business to the Top*. New York: Simon and Shuster 1996. pp. 186-200. see also, George Friedman, Meredith Friedman, Colin Chapman, and John S. Baker Jr., *The Intelligence Edge: How to Profit in the Information Age*. New York: Crown Publishers 1997. pp. 215-216, and James Adams, 1998. *The Next World War: Computers Are the Weapons & the Front Line is Everywhere*. New York: Simon & Schuster 1998. pp. 259-271.

<sup>50</sup> Sun Tzu, translated by Samuel B. Griffith.. *The Art of War* Toronto: Oxford University Press 1971. p. 101.

Figure 4 shows how the proposed IW-SWOT analysis integrates the Waltz information warfare model with the traditional SWOT analysis used by the business community. In this model, all three levels of Waltz’s information warfare model are examined for internal strengths and weaknesses as well as external threats and opportunities.

Figure 4 – IW-SWOT analysis



*Layer 1 - perceptual*

At the perceptual layer, the corporation must ask itself questions about how it is perceived by external actors. What are the opportunities and threats that the proposed venture entails? If the firm sees an opportunity to introduce a new product, enter a new market or form an alliance, is this obvious to other competitors, or does observing the opportunity rely on information that is closely held by the organization, for example, a newly-found application of an existing product? (If so, has this closely held information been compromised?) How is the firm perceived by competitors, customers, regulators,

non-governmental organizations? All of these groups have the potential to affect the firm's efforts. Competitors may try to hinder the firm's venture by casting it in a negative light. Customers may not trust the company's reputation. Regulators may try to institute new controls or may need to be persuaded to remove controls currently in place. Non-governmental organizations may object to the strategy on humanitarian or environmental grounds and try to affect the other groups or even target the firm directly through electronic or traditional means. To counter these threats, how might the firm better present itself to these groups?<sup>51</sup>

Internally, a different set of questions need to be answered. Are the facts and sources available to the firm reliable? What information is missing that is needed to make a better decision (gap analysis)? Is there a possibility of purposeful deception on behalf of a competitor? Are we effectively using the internal knowledge possessed by the firm?<sup>52</sup>

### *Layer 2 – infrastructure*

Here, the questions become more technological. The information infrastructure is the main area to be scrutinized, although some parts of the physical layer will be closely integrated. Are redundant network connections (i.e. more than one ISP) available? What are the regulatory requirements, and are they likely to change? What about the legal environment, for example, if the firm is selling or licensing intellectual property? Are

---

<sup>51</sup> These and similar questions may benefit from Benjanim Gilad's book, *Business Blindspots*. It is considered to be one of the best books on the market for setting up a competitive intelligence program.

<sup>52</sup> Jones, et al chapter 16 provides a thorough examination of integrating knowledge management with information warfare strategy in a corporate context.

there domestic laws against piracy or will the venture require a heavy reliance on technological piracy countermeasures?

Internal strengths and weaknesses must also be examined. Questions here may include: Is our information infrastructure readily adaptable to the new situation or will it require the purchase or development of adapting equipment/software? Are our security devices (e.g. IDS, PKI) scalable to cover the strategy? Are there inherent security weaknesses in the infrastructure, for example, using particular operating systems, software or applications? Are we vulnerable to denial-of-service attacks?

This layer will also require additional questions to be asked that cover both the internal and external environments, as they often rely upon each other. Centers of gravity must be identified and protected appropriately. Failure to do so may lead to cascading effects in the event of an attack.

### *Layer 3 - physical*

The physical layer must also be examined in light of centers of gravity and cascading effects. Externally, the firm needs to consider how robust the external infrastructure is. Are power outages common, and if so, how often do they occur? The answers may lead to the addition of secondary power generators. What about the local fire and policing organizations? Do non-governmental organizations pose a threat? Strategies involving foreign markets or competitors may also need to consider the possibility of wiretaps or TEMPEST attacks. Similarly, are the firm's assets vulnerable to directed energy weaponry?

Internally, physical questions such as the ability to store data must be examined. Does the firm have enough storage, processing power or bandwidth to support the strategy? How susceptible is the infrastructure to theft by insiders (i.e. laptop computers or easy access to cd/dvd burners)? Is physical sabotage a possibility?

This framework can also be used to help plan an organization's incident response / business continuity strategy. Crime also poses a risk to a firm's personnel, products, physical resources, and communications and information systems.<sup>53</sup> This framework may also be used to this end.

### Applying the IW-SWOT analysis

To see how this analysis framework may be applied to business strategy, it may be illustrative to examine it briefly in the context of two scenarios: (1) entering a foreign marketplace; and, (2) in the context of a hostile takeover.

#### *Entering a foreign market*

Suppose an American-based vendor of computer-based foreign-language courses decides that Cambodia is a market with great potential. The company sells CD-Rom based English lessons, and it has determined that Cambodians are eager to learn English to better participate in the global economy. Due to infrastructure constraints, the company has decided to sell its software pre-packaged through retail channels, rather than through its Web site. The strategy will require significant investment in warehouse space and setting up an in-country distribution company, and these investments represent opportunity costs. However, the financial models, market forecasts, and sensitivity

---

<sup>53</sup> Phil Williams, "Criminal Risk Assessment: A New Dimension of Competitive Intelligence." *Competitive Intelligence Review*. Volume 10, number 2, Q2 1999. pp.37-45.

analyses all indicate that this venture is of a medium-risk. Because the strategy involves intellectual property in a digital form, performing a IW-SWOT analysis is a prudent step.

The first layer is the perceptual layer. Externally, the firm should ascertain how it is perceived by the population. Are American companies scorned and the product's origins downplayed, or can the American origin of the lessons be used as a marketing opportunity (i.e. "Learn American English, the true language of international commerce. Forget the British and their talk of lorries, lifts, and scones. Learn the English spoken on Wall Street.")

The firm also needs to ask itself internal questions: How reliable are the data we used to arrive at the decision to pursue this strategy? Is there a potential for deception on behalf of competing firms? Are we making assumptions based on prejudices? Do we have any staff that have traveled or lived there and whose input we could use?

Next, the firm must address the infrastructure questions. Externally, the firm will be interested in the legal system and other infrastructure issues. It will need to address questions such as: How well do the Cambodian authorities deal with criminals who may try to pirate our product? How pervasive is corruption amongst government officials? Will we be able to find honest and reliable staff? Will we be at the mercy of telecommunications or power outages? Are there restrictions against using strong encryption for our VPN? Are we facing possible electronic penetration attempts from state-sponsored intelligence agencies?

Internally, infrastructure issues may include questions about the ability of the firm's information infrastructure to handle the new venture. How will the new employees or contractors be integrated into our data access system? What kinds of

permissions will they have and what level of authentication is needed? Can we use VOIP, or will this create a center of gravity in our communications infrastructure, as our data and voice will share the same network? How well will our anti-piracy technological countermeasures work?

Finally, physical questions need to be addressed. Externally, how well established are the shipping channels into the country and for internal distribution? Are we better off buying the raw materials locally and burning the CD-Roms and assembling the product there? How much of a threat does physical theft present?

Internally, questions may include: If we are manufacturing the product locally rather than importing them from the USA, how can we prevent unauthorized production runs from taking place? What kind of downtime can we afford, and how reliable will the available utilities be?

After considering these questions, many of which may have already been addressed, (albeit perhaps from a different perspective), the firm can make an assessment of what kind of risks information warfare tactics present to the strategy. This assessment may cause the strategy to be re-classified as a high-risk venture, especially if there is no strong answer to the piracy concerns.

*IW-SWOT in the context of a hostile takeover*

Suppose an American computer security software company, BigFish, Inc. is attempting to take over Minnow Industries, a manufacturer of token-based access controls and holder of a number of ground-breaking patents. The CEO of Minnow, and the inventor of its technology, has vowed to never work for BigFish, Inc. because

BigFish supplied database security for the DOD's controversial counter-terrorist database. The takeover will rely on the exchange of stock, and its likelihood of success is largely going to depend on the stock prices of the two companies. It is in the interest of both BigFish and Minnow to keep their stock price high while driving down the other firm's stock. Because stock prices are largely based on expectations (perceptions) of future profitability, the IW-SWOT model may be a useful tool to assess risk.

Both companies may engage in public-relations battles, much like those seen in the HP-Compaq merger of 2002. But the specter of information warfare tactics is also possible. BigFish may want to hurt the perception of Minnow, but not harm the underlying infrastructure – customers, intellectual property, etc. Minnow, on the other hand, may not have similar qualms about doing real damage in order to stave off the takeover. If BigFish were to be hacked and the source code of its next generation product were released, the hostile takeover may fail. This would be illegal of course, but the use of proxies should not be ruled out, especially given the controversy surrounding BigFish's DOD contracts. This threat could be even greater if it was learned that a foreign competitor was also interested in buying Minnow.

An IW-SWOT analysis may lead BigFish to conclude that it must realign its internal structures to better deal with the new threats posed by the situation. For example, BigFish may decide to start manning its IDS systems 24/7 rather than having its analysts examine the overnight logs in the morning. They may even go so far as to have a redundant system installed and monitored by outside experts. BigFish executives may be restricted from traveling overseas with details about the takeover stored on their notebook computers unless absolutely necessary (the principle of least privilege).

In this example, IW-SWOT is not used to chart out strategy, but may be used to assess the threats faced by the firm and allow it to shift its defensive countermeasures appropriately. While the solutions may seem to only affect the obvious weaknesses such as electronic intrusion, all three layers of the IW-SWOT model must be addressed in order to keep from overlooking the one vulnerability that allows an information warrior access.

The IW-SWOT analysis is thus a useful tool for assessing corporate strategy in light of the threats posed by information warfare tactics and the growing reliance of corporations upon their information infrastructure. However, this model is best suited to business operations. The other part of corporate strategy – the decision making process – needs to be addressed using a different approach. Information warfare tactics aimed at the decision making process are better assessed using the Denning model of information warfare.

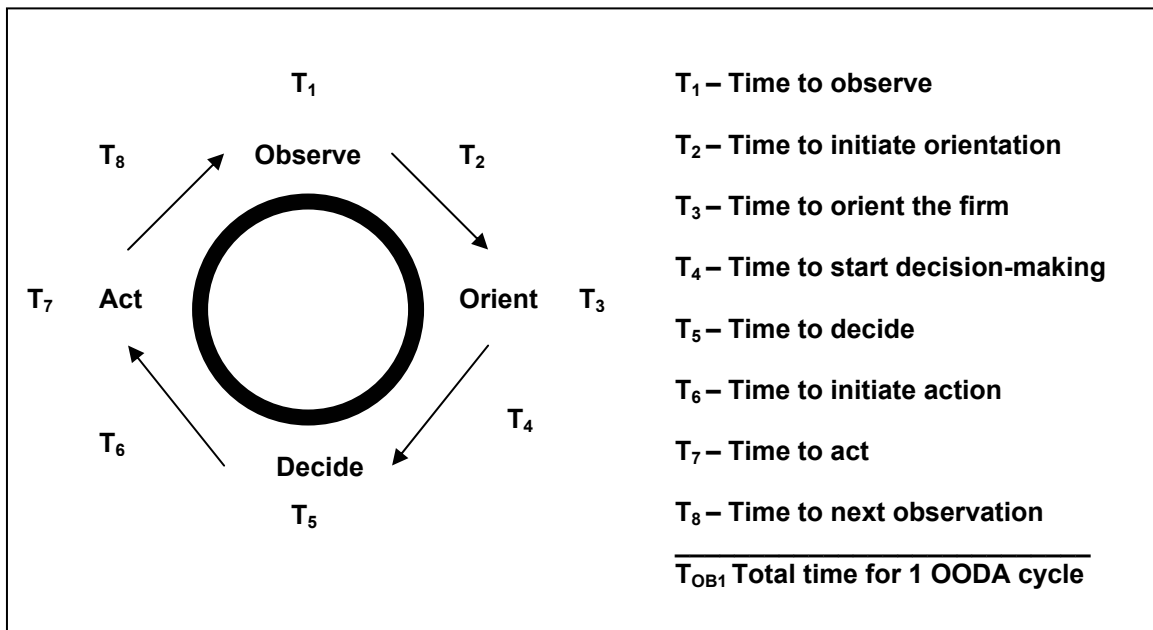
### The Decision Making Process and the OODA Loop

Corporations need to make decisions in a timely manner using the best data available. These decisions are also being made by their competitors, often using the same data and decision making processes. Here, the win-lose adversarial nature of the Denning information warfare model is appropriate because one firm's loss is another's gain. The firm that can best maximize the quality of data used and minimize the time needed to read, assess and make a decision has the advantage.

The OODA loop describes the decision making process. Originally developed by Air Force Col. John R. Boyd, this analysis of the decision-making process is gaining

popularity in business strategy.<sup>54</sup> It consists of four stages: (O)bserve – The observation that there is a business opportunity, or conversely, an impending threat to a firm’s strategy is the first stage of the decision making process; (O)rient – Here, the firm analyzes the situation; (D)ecide – This part of the loop is the time needed to weigh the options available to the firm; and, (A)ct – the time needed to implement the decision. These four stages are then repeated. OODA loops can be used to describe how a corporation may deploy a strategy, and then observe, orient, decide and act to make slight “tweaks” to the strategy. The OODA loop also describes how the process of recognizing a threat/opportunity or identifying a strength/weakness is conducted. OODA loops occur at all levels, from corporate-wide strategy to the toner re-ordering process.

Figure 5 – OODA loop<sup>55</sup>



At a tactical level, the OODA loop can be circumvented. One method is to cheat by doing the orientation and decision making processes first. Then, once a particular set

<sup>54</sup> Keith H. Hammonds, “The Strategy of the Fighter Pilot,” *Fast Company* June 2002. p. 98.

<sup>55</sup> Adapted from Nichols et al. pp. 477-480.

of circumstances is observed, a pre-determined set of actions takes place. The OODA loop is short circuited to exclude the orient and decision steps; it becomes a tight series of sequential observations and actions.<sup>56</sup> These processes are found today in automated stock trading programs and enterprise resource planning systems.<sup>57</sup> These systems rely heavily upon data sets and automated software processes, both of which are susceptible to information warfare tactics.<sup>58</sup> Corporations using such systems should use the IW-SWOT analysis described earlier to assess the threats to these systems.

This paper is concerned with corporate-level strategy, which most likely will involve situations where the OODA loop is used in its entirety. As noted in figure 5, there are 8 elements that make up one OODA loop. The corporation that is able to shrink the amount of time needed to complete an OODA loop has an advantage; as the loop shrinks, it can spin faster:

Businesses that execute decisions sooner than competitors will have the edge in influencing customers' perceptions and gaining market share. Rapid decision cycles enable a quick-to-market offering of modified or new goods and services.

This situational awareness permits you to understand what is influencing your organization and what influence you can wield. It also helps bring into focus what information you need to go after, as well as the IE (i.e., information, information infrastructure, and information-based processes) you need to defend. Concentrate your resources on the competition's essential elements of information (EIs) and your essential elements of friendly information (EEFIs). This traditional operations security (OPSEC) approach requires a thorough understanding of both your competition's and your own organization's IE, especially the value of information and critical processes.<sup>59</sup>

---

<sup>56</sup> Ibid., pp. 482-488. This short-circuited OODA loop is known as the Ryan Revision and described thoroughly in Nichols et al.

<sup>57</sup> Ibid., pp. 484-485.

<sup>58</sup> Joseph L. Bower and Thomas M. Hout. "Fast-Cycle Capability for Competitive Power." *Harvard Business Review* November-December 1988. pp.1-9.

<sup>59</sup> Jones, et al. pp. 473-474.

This application echoes that of Boyd himself. He describes the advantage gained by having an OODA loop that spins faster than an adversary's as 'operating inside' of the opponent's loop:

[O]perate inside adversary's observation-orientation-decision-action loops to enmesh adversary in a world of uncertainty, doubt, mistrust, confusion, disorder, fear, panic, chaos, ... and/or fold adversary back inside himself so that he cannot cope with events/efforts as they unfold.<sup>60</sup>

The process by which strategic decisions are made is the issue here. Unlike the IW-SWOT analysis, where the firm's susceptibility to information warfare tactics is used to help shape corporate strategy, here the Denning information warfare model can be applied to help a corporation operate inside an adversary's OODA loop.

The two critical elements are first, data, and second, the methods by which it is processed and acted upon. Here the tug-of-war aspects of the Denning model are more appropriate because of the adversarial relationship between corporations.

For information integrity, a robust defensive posture must be taken: the use of authentication, access control, monitoring, backups, and file integrity checkers are some of the methods that must be deployed. Offensive attacks on information integrity are generally illegal as they often involve legal or ethical violations. One exception to this, however, is the corporate use of disinformation. By seeding the perception of one's competitors with false or misleading information, one can reduce the integrity of the data set that the competition is reliant upon.<sup>61</sup> There are a number of ways that this can be done, however, the corporate use of disinformation can have serious repercussions. It can

---

<sup>60</sup> John R. Boyd, "Organic Design for Command and Control" Lecture May 1987. [Internet] available at <http://www.d-n-i.net/boyd/pdf/c&c.pdf>.

<sup>61</sup> John J. McGonagle and Carolyn M. Vella, *Protecting Your Company Against Competitive Intelligence*. Westport, CT: Quorum Books 1998. pp. 115-120.

cross the line of fraud if pushed too far. It may require one's own employees to be deceived, possibly corrupting the decision making process and harming morale. The corporation's credibility may be harmed. Finally, those in charge of the disinformation program may be adversely affected.<sup>62</sup>

The offense will try to gain as much information about the situation and the competition as possible. Again, many of the information warfare techniques that could be employed have serious legal or ethical hurdles, and as such will not be discussed here. One ethical and legal method though is the use of competitive intelligence.<sup>63</sup> Such a program, if properly implemented can increase the quality of data fed into the OODA loop, leading to better decisions. A legitimate competitive intelligence program must abide by a stringent set of ethics, such as those espoused by the Society of Competitive Intelligence Professionals (SCIP).<sup>64</sup> Information availability will require many of the same defensive countermeasures from an information assurance point of view as does information integrity. However, here again the corporation can take steps to protect itself, and unlike the use of disinformation, these countermeasures are ethical. The use of corporate "cloaking" programs is designed to monitor and minimize the amount of information leaked out to the world through regulatory filings, trade show exhibits, and

---

<sup>62</sup> Ibid., pp. 119-120. These four reasons are discussed in more depth by the authors.

<sup>63</sup> See Friedman et al, and Kahaner for details about setting up and running a competitive intelligence program.

<sup>64</sup> Kahaner, pp. 246-249. Describes the value of ethics, he cites an adage: *Eighty-five percent of the information you need is out there in the public domain; the other fifteen percent you probably don't need.* However, Pennenberg and Barry cite numerous examples of competitive intelligence professionals espousing one set of principles and abiding by another.

other such information sources that can be monitored by the competition's competitive intelligence operations.<sup>65</sup>

The Denning model is also useful to help ensure that the human resources involved in the decision-making process are able to fully contribute to the decision-making process. With the greater use of knowledge management techniques, a corporate decision-making team may operate in a "swarming" form of organization and rely upon an all-channel network – a network in which every node is connected to every other node in the network – format to ensure information and knowledge is accessible when it is needed.<sup>66</sup> These cutting-edge corporate teams will be susceptible to communications and coordination issues more so than their traditional counterparts.

### Conclusion

Global forces, such as those driving noopolitik, and an increased reliance on corporate information infrastructures suggest a change to the ways in which corporations formulate strategy. From an operational standpoint, information warfare threats should be assessed using a model such as the IW-SWOT model described in this paper. This model can be used to drive corporate strategy, especially in firms that deal heavily with information-based assets. Alternatively, the model can be used as a "sanity-check" for

---

<sup>65</sup> See McGonagle and Vella for a complete description of a cloaking program.

<sup>66</sup> John Arquilla and David Ronfeldt, *Swarming & the Future of Conflict* Santa Monica: RAND 2000. Defines 'swarming' as "seemingly amorphous, but is a deliberately structured, coordinated, strategic way to strike from all directions, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions," and points out that certain characteristics of the corporate infrastructure prevents businesses from truly swarming; however, the efforts that do approach the swarming model have the same vulnerabilities as those organizations that are truly able to swarm. See also John Arquilla and David Ronfeldt, "Networks, Netwars, and the Fight for the Future." *First Monday*. Volume 6, number 10, October 2001. [Internet] at [http://firstmonday.org/issues/issue6\\_10/ronfeldt/index.html](http://firstmonday.org/issues/issue6_10/ronfeldt/index.html). for a description of the characteristics of all-channel networks and the vulnerabilities they face.

more-traditional firms, such as those dealing with intellectual property or facing foreign competitors.

The decision making process is another area where information warfare models can be beneficial to corporate strategy. The OODA loop of corporate strategy development can be better protected by applying the Denning model of information warfare to the corporation's infrastructure. This model can also integrate competitive intelligence and counter-competitive intelligence programs in addition to the more familiar information assurance concepts.

## Bibliography

### *Books*

Adams, James. 1998. *The Next World War: Computers Are the Weapons & the Front Line is Everywhere*. New York: Simon & Schuster.

More of a discussion about military applications of information technology than a book on information security, Adams describes many new technologies and the interplay of government agencies in a post-cold war world. He dedicates an entire chapter to economic espionage.

Arquilla, John and David Ronfeldt. 2000. *Swarming & the Future of Conflict*. Santa Monica: RAND.

Swarming – a coordinated deliberate attack from all directions – is a strategy with a long history. Today’s ability to move information faster than ever before makes this form of combat easier to execute. Swarming techniques are seen today in the actions of NGOs. It is also present, to a lesser extent in military and business. The authors briefly discuss the aspects of business that are obstacles to the use of swarming as a business tactic.

\_\_\_\_\_. 1999. *The Emergence of Noopolitik: Toward an American Information Strategy*. Santa Monica: RAND.

Arquilla and Ronfeldt define ‘Noopolitik’ as “foreign–policy behavior for the information age that emphasizes the primacy of ideas, values, norms, laws, and ethics – it would work through ‘soft power’ rather than ‘hard power.’” Noopolitik concerns itself with cyberspace security and political strategy. Arquilla and Ronfeldt explain the reasons why we are seeing a shift in the power base away from nation-states and coercive military power to international organizations and the power of ideas. The underlying infrastructure of this change is, of course, the greater interconnectedness that modern technology allows, and thus, the protection of the information infrastructure is vital.

Boar, Bernard H. 1994. *Practical Steps for Aligning Information Technology with Business Strategies: How to Achieve a Competitive Advantage*. New York: John Wiley & Sons, Inc.

This book covers the history of IT, IT architecture, IT planning and forecasting, the economy, and does a rather good job in these respects. Notably absent is the mention of information security in any substantive form, even as a necessary part of a basic IT infrastructure. The author does not address the issues of confidentiality, integrity or availability with respect to information security. No attempt to use security posture as a competitive advantage or consider the possibility that particular IT choices may put a corporation at a disadvantage due to increased security vulnerabilities.

Collins, David J., and Cynthia A Montgomery. 1997. *Corporate Strategy: Resources and the Scope of the Firm*. Boston: Irwin.

This is an introductory textbook on corporate strategy by two Harvard business school professors. It covers SWOT analysis in addition to a number of other more specific strategies. Very dense and covers a number of strategic issues outside of the scope of this paper.

Denning, Dorothy E. 1999. *Information Warfare and Security*. New York: Addison Wesley.

A good overview of information warfare and security topics. Most notable is Denning's model of information warfare. In her model, she considers confidentiality and integrity to be opposite sides of the same coin, and describes issues of both confidentiality/integrity and those relating to availability as zero-sum gains between the offense and defense.

Friedman, George, Meredith Friedman, Colin Chapman, and John S. Baker Jr. 1997. *The Intelligence Edge: How to Profit in the Information Age*. New York: Crown Publishers.

An introductory book on the competitive intelligence industry. The authors discuss using open sources, especially Internet-based sources. The book also briefly describes how to protect an organization from the competitive intelligence programs of competitors.

Friedman, Thomas L. 1999. *The Lexus and the Olive Tree*. New York: Farrar, Strauss and Giroux.

The textbook for globalization 101, Friedman's book describes the modern economic forces of international commerce and their effects on the old (olive tree) and new (Lexus) worldviews. He also addresses to a lesser extent, how information technology comes into play, and how these forces combine to give rise to new threats to American interests.

Gilad, Benjamin. 1996. *Business Blindspots 2<sup>nd</sup> Edition*. Wiltshire, England: Infonortics

This book is often cited as the best single source for information on the competitive intelligence process. Laden with examples, this well-researched book presents a framework for collecting and using information in the enterprise.

Jones, Andy, Gerald L. Kovacich, and Perry G. Luzwick. 2002. *Global Information Warfare: How Businesses, Governments and others Achieve Objectives and Attain Competitive Advantages*. Boca Raton: CRC Press.

The authors show a deep understanding of information warfare concepts and how these techniques are applied by nation states, non-state actors, and corporations. They discuss the OODA loop in a business context and discuss knowledge management as a defensive tool.

Kahaner, Larry. 1996. *Competitive Intelligence: How to Gather, Analyze, and Use Information to Move Your Business to the Top*. New York: Simon and Shuster.

An overview of the competitive intelligence process; the author covers collecting, analyzing, and disseminating intelligence, benchmarking, and how foreign governments are involved in the competitive intelligence/corporate espionage game.

Lewis, Michael. 2000. *The New New Thing: a Silicon Valley Story*. New York: W. W. Norton & Company.

An entertaining account of a boy and his boat, in this case CGI/Netscape/Healthscape founder Jim Clark and his übertoy: *Hyperion*. This book is illustrative tale about the beginning of the dot com

boom/bust and the competition between high tech companies; notable for its account of the Microsoft antitrust case's origin.

McCarthy, Mary Pat, and Stuart Campbell with Rob Brownstein. 2001. *Security Transformation: Digital Defense Strategies to Protect Your Company's Reputation and Market Share*. New York: McGraw-Hill.

This is a poorly researched computer security book that covers the basics of information security with barely enough material on business to justify the title. It discusses security as a part of corporate strategy, but only on a superficial level.

McGonagle, John J., and Carolyn M. Vella. 1998. *Protecting Your Company Against Competitive Intelligence*. Westport, CT: Quorum Books.

This book describes how to implement a corporate “cloaking” program designed to shield a corporation's strategic plans from being deduced by outsiders through the use of competitive intelligence. Also discusses other techniques such as avoiding revealing information while talking on cellular phones or when researching competitors on the Internet. An appendix discussing the corporate use of disinformation is also quite enlightening.

Nichols, Randall K., Daniel J. Ryan, and Julie J.C.H. Ryan. 2000. *Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves*. New York: McGraw-Hill.

Authors cover a broad variety of information security topics, with a focus on integrating various disciplines into a comprehensive information security program. The decision-making process and OODA loop is covered in depth, including a description of next-generation OODA loop models.

Penenberg, Adam L. and Marc Barry. 2000. *Spoaked: Espionage in Corporate America*. Cambridge: Perseus Publishing.

This book gives a cursory view of the competitive intelligence/corporate espionage industry, and includes a chapter on the role of hacking in corporate espionage. The authors are a journalist and a competitive intelligence practitioner.

Rattray, Gregory J. 2001. *Strategic Warfare in Cyberspace*. Cambridge: MIT Press.

A dense and thorough explanation of information warfare and its larger strategic context. Rattray describes the challenges for both offensive and defensive information warfare and uses the development of U.S. strategic airpower as a historical example of developing the strategic warfare capabilities of new technology.

Stiglitz, Joseph E. 2002. *Globalization and its Discontents*. New York: W.W. Norton & Company.

Stiglitz presents an argument that the IMF does more harm than good when it intervenes into national economies, and gives insight into the resentment of the West by those countries that the IMF has “helped.” This book is a good compliment to *The Lexus and the Olive Tree*.

Tzu, Sun, translated by Samuel B. Griffith. 1971. *The Art of War*. Toronto: Oxford University Press.

This Chinese war manual is a classic tome whose prescience is perhaps overshadowed by its overexposure in pop culture.

Waltz, Edward. 1998. *Information Warfare Principles and Operations*. Boston: Artech House.

Waltz presents a comprehensive and well thought out model of information warfare. Presented as a manual for gaining superiority in a battles infospace, Waltz addresses the direct and indirect effects of information warfare at the perceptual, information infrastructure, and physical levels.

Winkler, Ira. 1997. *Corporate Espionage: What it is, Why it's happening in your company, What you must do about it*. Rocklin, CA: Prima Publishing.

The author has written an excellent treatise of the nature and extent of corporate espionage. Winkler describes espionage concepts, provides case studies and makes recommendations. The recommendations section of the book is extremely valuable and should be consulted when designing an information security program.

### *Journal Articles*

Arquilla, John and David Ronfeldt. 2001. "Networks, Netwars, and the Fight for the Future." *First Monday*. Volume 6, number 10, October 2001. [Internet] at [http://firstmonday.org/issues/issue6\\_10/ronfeldt/index.html](http://firstmonday.org/issues/issue6_10/ronfeldt/index.html).

This essay is an updated version of chapter 10 in their book, *Networks and Netwars*. The Authors describe how new forms of organization have historically been first exploited by 'bad guys' and how chain, hub and all-channel networks function. They describe the strengths and weaknesses of such networks and discuss the challenges hierarchical organizations face when battling network-based adversaries.

Beeson, Jim. 1993. "Riding the Marketing Information Wave." *Harvard Business Review*. September-October 1993. pp. 150-160.

Information technology is allowing large corporations to market to their customers with levels of personalization that had previously only been achievable by smaller, niche companies. This customization relies heavily on information systems and large customer databases. The article also addresses the privacy issues surrounding the sharing of customer information.

Bocij, Paul. 2002. "Corporate Cyberstalking: An Invitation to Build Theory." *First Monday*. Volume 7, number 11, November 2002. [Internet] available at [http://firstmonday.org/issues/issue7\\_11/bocij/index.html](http://firstmonday.org/issues/issue7_11/bocij/index.html).

An examination of stalking behavior on the Internet; the author proposes a typology for cyberstalking that includes individuals stalking corporations, corporations stalking individuals, and corporations stalking other corporations.

Bowler, Joseph L., and Thomas M. Hout. 1988. “Fast-Cycle Capability for Competitive Power.” *Harvard Business Review*. November-December 1988. pp. 1-9.

The authors describe “fact-cycle” companies – those companies that use information technology and new organizational structures to reduce the amount of time needed to make decisions. Fast-cycle time is described as playing two roles: (1) as a way for designing an organization with the goals of improving speed and efficiency as well as providing faster response to changing market demand and competitive activity; and, (2) a way of organizing and leading a company with the goal of gaining a real advantage over the competition. The OODA loop is briefly mentioned, and the authors describe how fast-cycle processes help organizations save time and improve service as they sell Toyotas, telephones, fabrics, fashions or loans. The authors note that these fast-cycle companies are more dependent upon information infrastructures, but fail to mention that such a posture exposes companies to technological vulnerabilities.

John R. Boyd, *Organic Design for Command and Control*. May 1987. [Internet] available at <http://www.d-n-i.net/boyd/pdf/c&c.pdf>.

Part of Boyd’s lengthy “Discourse on Winning and Losing,” this series of slides describes how reliance on technology is misguided and that people and ideas should be taken into account before relying upon technological solutions. Boyd addresses the challenges of preventing chaos from variety and rapidity while simultaneously preventing uniformity, predictability and non-adaptability that often results from harmony and initiative. He states that orientation is the most important part of the OODA loop because it shapes how we observe, decide and act. The series of slides shows Boyd’s in-depth understanding of history and the importance of new ideas.

Cronin, Blaise, and Holly Crawford. 1999. “Raising the Intelligence Stakes: Corporate Information Warfare and Strategic Surprise.” *Competitive Intelligence Review*. Volume 10, number 3, Q3 1999. pp. 58-65.

This paper describes the importance of intelligence to management with respect to business strategy. The authors also describe how a lax security posture can betray efforts to keep strategic plans secret, undermining new ventures or alliances.

Delargy, K.M. 2001. “The New Business Landscape.” *Manufacturing Engineer*. Volume: 80 Issue: 4, Aug. 2001. pp. 169 -174.

Author argues that business and technology strategies must be planned together in order to take full advantage of the new forms of collaboration that new technologies make possible.

Heuer, Jr., Richards J. 1981. “Strategic Deception and Counterdeception: A Cognitive Systems Approach.” *International Studies Quarterly*. Volume 25, Issue 2, June 1981. pp. 294-327.

A dense study of the way in which deception can be perpetrated and detected; the author describes how predetermined notions affect the effectiveness of various approaches.

Johnson, David R., and David Post. 1996. “Law and Borders – the Rise of Law in Cyberspace.” *First Monday*. Volume 1, number 1, May 6, 1996. [Internet] available at <http://www.firstmonday.org/issues/issue1/law/index.html>.

An interesting and thoughtful discussion of the nature of internet communication and the applicability of law, which is traditionally tied to authority based on the physical domain, to such transborder problems such as trademark infringement, defamation law, net-based professional activities, fraud and antitrust, copyright law. The authors suggest that treating cyberspace as a separate place for purposes of legal analysis will simplify and facilitate the application of law.

Kauffman, Robert J., Tim Miller, and Bin Wang. 2002. "When Internet Companies Morph: Understanding Organizational Strategy Changes in the 'New' New Economy." *First Monday*. Volume 7, number 7, July 2002. [Internet] available at [http://firstmonday.org/issues/issue7\\_7/kauffman/index.html](http://firstmonday.org/issues/issue7_7/kauffman/index.html).

A study of 125 Internet based companies and the various strategic techniques attempted to improve viability. Strategies included adjusting product offerings for an existing customer base, moving upstream to address a more profitable customer base, adjusting price models, or pursuing an offline presence.

Loch, Karen D., Houston H. Carr, and Merrill E. Warkentin. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding." *MIS Quarterly*. Volume 16, number 2, June 1992, pp. 173-186.

This paper documents a survey of information managers and finds the group to be lagging in their understanding of the nature and scope of the threat posed to their organizations by computer viruses.

McCullagh, Adrian. 2002. "Management Responsibility in Protecting Information Assets: An Australian Perspective." *First Monday*. Volume 7, number 7, July 2002. [Internet] available at [http://firstmonday.org/issues/issue7\\_7/mccullagh/index.html](http://firstmonday.org/issues/issue7_7/mccullagh/index.html).

The author examines the question of managerial liability in regard to the implementation of appropriate information security safeguards. She examines the duties to the shareholders of the organization as well as the potential for liability in the event corporate assets are used against third parties.

Muncaster, G. and E.J. Krall. 1999. "An Enterprise View of Defensive Information Assurance." *Military Communications Conference Proceedings, 1999*. IEEE 1999, Volume 1, 1999. pp. 714 -718.

The authors describe Motorola's Defensive Information Assurance (DIA) program. This program integrates Risk Management, Systems Integration, Resource Management, Electronic Warfare, and conventional Defensive Information Warfare tactics in a System of Systems model. The authors argue this approach is needed to cover the shortcomings of traditional Defensive Information Warfare efforts.

Reicheld, Frederick F., and Phil Schefter. 2000. "E-Loyalty: Your Secret Weapon on the Web." *Harvard Business Review*. July-August 2000. pp.105-113.

An examination of repeat customers and the correlation to profitability in e-commerce firms, the authors conclude that a repeat customer base is critical to running a profitable e-commerce business. They also conclude that the trust relationship that exists between customers plays a greater role online than in the real world.

Schell, R.R. 2001. “Information Security: Science, Pseudoscience, and Flying Pigs.” *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*, 2001. pp. 205 -216.

The author offers a well-thought critique of modern information security, especially the accreditation methods used today. He correctly points out that today’s methods – such as penetration testing – prove the existence, not the absence of flaws.

Singh, Tejinder, Rajan Subramanian, and Tripatinder S. Chowdhry. 1990. “Impacts of Future Information Systems on Business Strategies.” 1990 IEEE International Engineering Management Conference.

The authors discuss how emerging communication technology is being used by businesses to save money. They recommend that business managers pay attention to the greater risks inherent in deploying these systems internationally and take steps to ensure their communications are not compromised.

Tractinsky, Noam, and Sirkka L. Jarvenpaa. 1995. “Information Systems Design Decisions in a Global versus Domestic Context.” *MIS Quarterly*. Volume 19, number 4, Dec. 1995. pp.507-534.

The authors surveyed two groups of IT managers - one group with domestic experience and one group with international experience - about the importance of various IT issues. The goal was to determine if managing IT in a global context differed from managing IT domestically.

Williams, Phil. 1999. “Criminal Risk Assessment: A New Dimension of Competitive Intelligence.” *Competitive Intelligence Review*. Volume 10, number 2, Q2 1999. pp.37-45.

The author argues that corporate intelligence units be tasked with criminal threat assessment in order to improve risk management analysis. He breaks threats into those against personnel, products (e.g. counterfeiting), physical resources, communication and information systems, and threats from business partners. While the acknowledgement of information-based threats is a positive development, he neglects to consider information-based attacks on products.

### *News Articles*

Cavallaro, Michaela. 2001. “Tunnel Burns, Internet Melts.” *The Industry Standard*, July 20, 2001. [Internet] at <http://www.thestandard.com/article/0,1902,28110,00.html>, accessed November, 30, 2002.

A newspaper article describing the widespread effects that occurred after a train caught fire in a Baltimore tunnel and destroyed the fiber optic link that was using the tunnel as a conduit.

Chambliss, Lauren. 2002. “Hiring ‘Big Gun’ hacker backfires on Murdoch.” *The Evening Standard (London)*. October 10, 2002. p. 41.

A newspaper account of the hacker hired by News Corporation and the allegations that he helped pirate a competitor's satellite TV system.

Hammonds, Keith H. 2002. "The Strategy of the Fighter Pilot," *Fast Company* June 2002. p. 98.

An article about Col. John R. Boyd and how his theories on decision-making and strategy, including the OODA loop, are being used by businesses to compete with one another. Well written and entertaining, this article is a good introduction to Boyd's character and theory.

Harding, James, and Raphael Minder. 2002. "Rivalry erupts in lawsuit over digital television code." *Financial Times (London)*. March 13, 2002. p. 26.

A newspaper account of the accusations against News Corporation that the company provided expertise to help counterfeiters foil a competitor's smart card security features.

Lemos, Robert. 2001. "Rental-car firm exceeding the privacy limit?" *Tech News – Cnet.com*. June 20, 2001. [Internet] at <http://news.com.com/2100-1040-268747.html?legacy=cnet>

This article describes the efforts of one rental car company to fine its customers when they break the speeding limit in one of the company's vehicles. The firm uses GPS technology to track its fleet.

Newman, Judy. 2002. "Telecom Companies Use Ad Blitz: SBC Ameritech Isn't Happy Letting Other Companies Use Its Lines." *Wisconsin State Journal*. November 1, 2002. p. E1.

A newspaper account of the people and corporations behind the "Voices for Choices" television campaign.

Ross, Rachel. 2001. "DirectTV Move KOS Bootleg Access Cards." *The Toronto Star*. January 30, 2001.

A newspaper account of the Hughes Electronics attack on counterfeit satellite TV cards.

Stewart Thomas A. 2001. "America's Secret Weapon." *Business 2.0*, December 2001, pp. 58-68.

A business magazine article on how management theory is being used by thinkers like John Arquilla to help fight the war on terror.