Why Environmental Scanning Methods Work Except When You Need Them: The Threats of Asymmetric Attacks and Strategic Inflection Points

Introduction

> *"Big men don't scare easy."*
> *"Big men get popped off regularly."*
> - William Conrad (racketeer Castro) and Dick Powell (ex-con Rocky Malloy) in *Cry Danger*[1]

We can handle today, but tomorrow keeps us awake at night. Maybe that's a good thing; some of the top business people in the country seem to be running scared. Intel's chairman Andrew Grove even says he finds fear healthy, "It is fear that makes me scan my e-mail…makes me read the trade press…gives me the will to listen to the Cassandras...fear can be the opposite of complacency" Bill (Sleepless-in-Seattle) Gates says that he expects Microsoft to have to weather at least three major crises in the next ten years and (if that were not bad enough) that, "One day an eager upstart will put Microsoft out of business. I just hope it's fifty years from now, not two or five."

So why are these guys so worried? Surely companies as large and powerful as Intel and Microsoft could not be put out of business in two to five years. Surely they have developed environmental scanning "radar systems" to warn their Titanic enterprises about the icebergs on the horizon. Maybe they have, but then the original Titanic wasn't sunk by an iceberg. An iceberg didn't ram the Titanic; the Titanic rammed an iceberg. Environmental scanning systems are like the spotters in the Titanic's crow's nest; they can only warn about the type of attack that is expected: icebergs; they cannot warn about the real but unexpected threat: excessive speed given the turning radius of such a huge ship.

Expected attacks (however unpleasant) are not going to sink a Microsoft. Expected attacks are part of the current industry game, a game the Microsofts of this world have been consistently winning or they wouldn't be where they are. Asymmetric or unconventional attacks, on the other hand, mean the game has changed and that the Microsofts are as amateurish and as likely to lose as any other player. They may be even more likely than their attacker to lose since in the short run they must play the attacker's game. In the short run the attacker has what the military calls "the initiative."

Bill Gates may be especially worried because nobody in business should understands the danger of asymmetry better than he does. Gates came out of nowhere to take on, and in may ways defeat, IBM which was probably the best run Blue Chip company of the time. Later Gates was nearly the victim of an asymmetric attack by the internet-oriented firms such as Sun.

But asymmetric attacks are relatively uncommon so environmental scanning probably works most of the time, right? Not necessarily. There is still the situation in

[1] Quotes at the beginning of sections are from *Hard Boiled: Great Lines from Classic Noir Films* by Peggy Thompson and Saeko Usukawa.

which the danger is detected, but the necessary course of action is so painful the firm suffers a paralysis of will during which it fails to do anything. Grove defined strategic inflection points as places where businesses experience quantum changes in the balance of the current competitive environment. In this situation he says that the main problem is a sort of corporate cognitive dissonance: top managers know what they need to do, but can't even bring themselves to say the words much less take the steps.

This paper looks at two threats: asymmetric attacks and strategic inflection points. It will be argued that environmental scanning systems are useless in the face of the former (since their approach cannot be detected) and nearly useless in the face of the latter (since, although their approach can be detected, management will generally lack the will to respond to the warning).

The next two sections define and explain asymmetric attacks and strategic inflection points respectively. A discussion of environmental scanning systems follows that; the first of three sections shows how those systems are supposed to work, the second shows why they tend to fail in general, and the third shows why they tend to fail in the specific case of an asymmetric threat. The paper ends with two sections with advice for dealing with strategic inflection points and asymmetric threats respectively followed by general conclusions.

What is an Asymmetric Attack?

> "*My, my. Such a lot of guns around town and so few brains.*"
>
> - Humphrey Bogart (private eye Philip Marlowe) in *The Big Sleep*

The U.S. Army may be the 900-pound gorilla of the world's armies, but its deep thinkers in War College's Strategic Studies Institute (SSI) are nevertheless very concerned about what they recently began to call "asymmetric" attacks. The term "asymmetry" first appeared in military strategy literature in 1995 (although the concept goes back to ancient times). Since '95' the definition of asymmetry has evolved from the somewhat fuzzy "not fighting fair" to the more specific "acting, organizing, and thinking *differently* than opponents in order to maximize one's own advantages, exploit an opponent's weaknesses, attain the initiative, or gain greater freedom of action."

The standard (non-asymmetric) attack is like a boxing match in which two people hammer away at each other using about the same methods and technology; not surprisingly the big guy usually wins. In an asymmetric attack the smaller guy pulls out a gun. September 11, was an asymmetric attack; al-Qaida didn't box according to the Marquis of Quensbury Rules.

One should not infer from the September 11 example that a competitor's use of asymmetry is always deliberate. The SSI notes that, "More often, antagonists in a conflict or war simply use what they have and do what they know how to do. That the outcome is asymmetric is more accidental than planned." Thus the definition of asymmetry allows for fortuitous (even inadvertent) success.

Successful inadvertent asymmetric attacks are common in war. Americans fought the British and the Communist Chinese fought the Nationalists using asymmetric guerilla tactics, but in both cases the success and the use of that approach probably had as much to do with necessity and luck as with clever thinking.

Although the military definition of asymmetry covers inadvertency, it is still too narrow for business strategy purposes in that it assumes a human enemy. Businesses are more fragile than armies and can be destroyed merely by the flow of history; for example, the makers of buggy whips went out of business simply because time had passed them by. The definition of an asymmetry used here captures both the possibilities of inadvertency and of attacks not caused by a human enemy.

In this paper asymmetry is "any major change in the forces in the competitive environment that substantially reduces a firm's strategic advantages, or increases its strategic disadvantages either absolutely or in comparison with its real competition." There are two issues of special importance in this definition. The first is that the word change is being used here as it is when one talks about changing a tire or changing clothes. A ***change*** in the forces in the competitive environment means a new force has arrived, an old force has left, or both; this is more than just a change in the level or balance of ***existing*** forces. Major changes in the competitive environment that only involve the level or balance of existing forces are called strategic inflection points (which will be discussed in the next section).

The second issue of importance in the definition of asymmetry is that the relative change in a firm's strategic advantages or disadvantages is vis-à-vis its ***real*** competition. The real competition may not be the same as the perceived competition. Al-Qaida has only been widely recognized as one America's real competitors since September 11, but of course they have been one of the country's real competitors for quite some time.

As the world changes faster and faster asymmetric attacks (inadvertent or intended) are becoming more and more common in business. Mintzberg notes that the opinion of 1960s-era business writers such as John Kenneth Galbraith that giant corporations were relatively free from any serious competition seems quaint and ridiculous given recent history. Galbraith might have also said the same thing about the American military and he would have been just as wrong. He expressed his outdated notion in the last decade in which it may have seemed true, before the Japanese car manufacturers turned manufacturing giant GM into one of the biggest money losing enterprises in history, before Big Blue's share of the computer industry was dramatically cut by whiz kids like Steven Jobs with "toy" computers they built in their garages, and before the U.S. lost the war in Vietnam.

Just as the Colt 45 was the "great equalizer" in the old west, new technologies like the internet have equalized the business playing field today; companies like Amazon.com have used the internet to come out of nowhere launching asymmetric attacks on companies many times their size. The days of the smug/secure corporation are long gone.

Asymmetric attacks are like mutations in nature; they are generally unsuccessful, but when they do succeed, the results can be devastating for preexisting species. The bad news is that asymmetric threats not only present the biggest danger to the otherwise secure firm, but (as will be argued later) their approach cannot be detected by environmental scanning systems.

As the next section shows, the situation with respect to strategic inflection points is only marginally better. While environmental scanning systems can spot them, management may still be unwilling to do anything about them.

What is a Strategic Inflection Point?

> *"Why didn't you come home before?"*
> *"Why didn't I go to China? Some things you do, some things you don't."*
> - Keith Andes (fisherman Joe Doyle) to Barbara Stanwyck (his sister) in *Clash by Night*

Why did Microsoft fail to make internet application development their number one priority by the beginning of 1995? Why did Intel doggedly stick with making memory chips when they knew the Japanese were on the verge of eating their lunch? Were Microsoft and Intel suffering from the same sort of blindness? It doesn't seem that they were. Microsoft was faced with an asymmetric threat. The forces in the computing world had changed; the importance of the Internet was new and therefore something that environmental scanning systems cannot see. Intel, on the other hand, was faced with a strategic inflection point. Their environmental scanning systems had detected the Japanese threat, but management simply could not bring themselves to deal with it…they didn't do anything.

The distinction between not being able to see and refusing to see may seem academic. In a popular science fiction series, spaceships were made invisible by cloaking them in a "somebody-else's-problem" field; since people refuse to see somebody else's problem, the ships were just as invisible as if they were really "invisible." Thus, strategic inflection points which management doesn't want to see are nearly as dangerous as asymmetric threats which they can't see.

Grove defines a strategic inflection point as the point "when the balance of forces shifts from the old structure, from the old ways of doing business and the old ways of competing, to the new." The forces to which he refers are Porter's 5 forces (existing competitors, customers, suppliers, new entrants, and substitutes) augmented by Grove's new force of complementors (businesses from which our customers buy products that either work better or only work with our product). Strategic inflection points are less dangerous than asymmetric attacks since they only involve changes in the levels of existing forces rather than changes in the forces themselves (although the changes are very large…Grove says ten times or "10 X"). They are also less dangerous in that their approach is usually much slower but still may be hard to identify; as Grove warns, "They build up force so insidiously that you may have a hard time even putting a finger on what has changed, yet you know that something *has.*"

Fortunately, environmental scanning systems are designed to pay attention to these six forces and should, therefore, recognize strategic inflection points. Unfortunately, according to Grove, management will still have a very difficult time deciding to deal with the threat. This lack of a will to react is illustrated by Intel's experience with memory chips.

Intel began business as a memory chip company, but the Japanese slowly changed the rules of the game eventually devoting far more resources to memory chip development and production processes than any American player. Grove admitted that he and his lieutenants refused to really look at the painful new world. It was simply unthinkable for Intel, a "memory chip maker", to consider a future in which they did not make memory chips. Finally, considering an even more disturbing image of a future in which they had been fired for mismanagement, they began to wonder what their successors would do. The answer was obvious: they'd get out of memory chips. This realization jogged Grove out of his slumber. He realized that if his successor could make such a bold move, so could he.

Grove seemed genuinely surprised that he had to go that far in his thinking (to the extreme of putting himself in his successor's shoes) to be able to see what should have been obvious. It wasn't as if the Japanese memory chip attack was sudden and unexpected…this wasn't Pearl Harbor. In fact, Intel was already aware of the Japanese as competitors in the late 1970s, they even used the Japanese producers as subcontractors when caught short of production capacity. It took nine long years for the Japanese share of the worldwide semiconductor market to grow from about 28% (in 1976) to the point where it equaled the US share of about 45% (in 1985).

Maybe Intel could have done something during those years, but they didn't. Intel was a frog sitting in water that had very slowly been brought to a boil. By 1984 it was crystal clear that the water was much too hot and Intel would have to abandon the memory business, but it wasn't until the middle of 1985 that Grove finally made up his mind to take the company in that direction.

The difference between this strategic inflection point and an asymmetric attack is that it was both detectable and (in fact) detected. Environmental scanning systems at Intel did what they were supposed to do by identifying the Japanese threat, but despite that they were nearly ineffective because the will to act on the information was still lacking.

Although the discussion so far suggests problems with environmental scanning systems, nothing has yet been said about how these systems are supposed to work and why they are likely to fail. The next three sections take up these issues. The next section describes how environmental scanning systems are supposed to work and the two sections following that describe respectively why they fail in general and why they fail in the specific case of an asymmetric threat.

How Are Environmental Scanning Systems Supposed to Work?

> *"Maybe she was all right, and maybe Christmas comes in July. But I didn't believe it."*
>
> - Humphrey Bogart (war vet Rip Murdock) in *Dead Reckoning*

In order to better appreciate the problems environmental scanning systems have with asymmetric threats and strategic inflection points it is necessary to step back and consider how these systems are supposed to work. Environmental scanning according to Thompson and Strickland (1998) "involves studying and interpreting the sweep of social, political, economic, ecological, and technological events in an effort to spot budding trends and conditions that could become driving forces." While those authors admit that environmental scanning is "highly qualitative and subjective" they nevertheless offer some analytical approaches for dealing with it, such as constructing scenarios, and answering questions such as the following (which seem to roughly correspond to what most people have in mind when they talk about environmental scanning):

1. What are the industry's dominant economic features?
2. What is competition like and how strong are each of the competitive forces?
3. What are the drivers of change in the industry and what impact will they have?
4. Which companies are in the strongest/weakest positions?
5. What strategic moves are rivals likely to make next?
6. What are the key factors for competitive success?
7. Is the industry attractive and what are its prospects for above-average profitability?

Proponents of environmental scanning also usually recommend that these questions be answered by dedicated strategic planers, staff people removed from day-to-day operations so they can concentrate on the big picture. The use of analytical systems (such as these 7 questions) and the use of dedicated strategic planners are the root causes of environmental scanning system failure as the next two sections will illustrate.

General Problems With Environmental Scanning Systems

"I came to Casablanca for the waters."
"But we're in the middle of the desert."
"I was misinformed."

- Humphrey Bogart (nightclub owner Rick) and Claude Rains (Capt. Louis Renault) in *Casablanca*

Mintzberg (1994) wrote about problems in strategic planning in general, but the problems he saw with that task are all on point for environmental scanning (which is a part of strategic planning). Mintzberg reduces his criticisms of strategic planning (and thus of environmental scanning) to three fallacious assumptions.

Mintzberg first argues that environmental scanning systems will fail because analytical systems (like the above seven questions) are designed to break information into pieces while what is needed is just the opposite: something to synthesize (or assemble) the pieces into a meaningful whole. Mintzberg insists that a line manager's intuition is the only thing known to be capable of synthesizing both a clear picture of the situation and then a strategy for dealing with it.

Thus, the first fallacious assumption he identifies is: the "assumption of formalization", the belief that systems can be made to generate intuitions on par with those of line managers. Mintzberg says that this assumption is based on a misunderstanding of Taylorism (the approach to specifying the "one best way" of doing anything). He reminds us that Taylorism requires an understanding of the process to be formalized and since no one understands the workings of a line manager's intuition, those workings cannot be formalized.

The second fallacy that Mintzberg identifies is the assumption of detachment, the belief that "thought must be detached from action, strategy from operations, ostensible thinkers from real doers, and therefore, 'strategists' from the objects of their strategies." As already noted, the conventional view is that strategies are to be made by expert planners not bogged down in the day-to-day operating of the company. Theses experts would also be the ones to try to determine the meaning of data from the environmental scanning system. Mintzberg argues that such experts are no better than the systems they are using since both lack the line manager's intuition.

The third fallacy according to Mintzberg is the assumption of predetermination. For the wider topic of strategic planning this fallacy is the belief that the strategy making process can be specified in advance of making strategy and that the consequences of a strategy can likewise be determined in advance of its implementation "because the context for strategy making is stable, or at least predictable." Mintzberg argues that strategies are often incorrectly relied upon as road maps "with a fixed and well-defined target, as well as the steps to reach that target."

For the narrower topic of environmental scanning the third fallacy is especially problematic where one-time events are concerned (a problem that will be discussed further in the next section). The competitive situation in business is more unstable than it has been in the past and one-time events are more and more common. Mintzberg notes this fact and points out the irony that the more the world changes the less accurate predictions can be, but despite that (or maybe because of that) the more anxious business people are to have them.

The fallacious assumptions discussed in this section relate to both asymmetric attacks and strategic inflection points. However, there is more that should be said about the specific problem of scanning for asymmetric attacks. That is the subject of the next section.

Environmental Scanning Problems Specific to Asymmetric Threats

There are many problems with the seven questions used in environmental scanning as far as asymmetric threats are concerned. These problems should be more obvious now in the light of Mintzberg's objections. First, as already noted, there is nothing in the questions nor in the expert strategists who are supposed to answer them which will cause a picture of the future to be synthesized (the fallacy of formalization). Questions 1, 2, 4, and 6 all are oriented toward considering the *status quo* which is apparently assumed likely to be maintained (the fallacy of predetermination). Even if the people at Microsoft had answered those four questions in 1995 (and they probably did), it is hard to believe that their answers would have been useful in identifying the completely new threat of the internet. Questions 3, 5, and 7 are better in that they more oriented towards the future, but it hard to say how they would work for a company facing a fundamental shift in their industry; question 3 seems especially problematic. What would be the use of identifying drivers of change in the industry when the changes are coming from outside the industry? Question 5 would be irrelevant since first, the firm's perceived rivals would most likely not be their real rivals and second, the perceived rivals are in the industry and would be just as clueless about what course of action to take as is the firm itself. Question 7 assumes the firm knows what "the industry" means; again this is unlikely since the industry has changed. The seven questions would, of course, be more likely to generate useful answers where the company is facing a strategic inflection point, but in that case the issue still remains as to whether or not management would be willing to act on what they learn.

Mintzberg points out that predicting (scanning for) one-time events (such as the asymmetric attack on the World Trade Center and Pentagon) is nearly impossible since there are no patterns or causal relationships from which to construct a model. We can only predict the weather because the same sort of weather happens over and over again. It is perhaps now possible to set up an environmental scanning system to warn of an impending September 11-like attack on a tall building somewhere; we know (for example) that it might be a good idea to monitor foreign nationals enrolled in domestic flight schools. But such an attack would no longer be truly asymmetric because it would no longer represent a real change in the competitive environment.

The difficulty in scanning for one-time events is shown in Gates (1999) which describes how hundreds of analysts in the computer industry got their predictions wrong not once but twice in 1995. He relates how newspaper and magazine headlines in 1995 went from mistakenly declaring Microsoft "invincible" in August (due to the successful rollout of Windows 95) to again mistakenly saying Microsoft "didn't get it" (the "it" being the Internet) only two months later. Microsoft stock was actually downgrade by Goldman Sacks in mid-November.

Microsoft was very-nearly the victim of the fast-moving asymmetric attack of the internet in 1995. The attack wasn't the result of any (at that time) currently identified force in the personal computer software industry. The attack was not caused by the existing rivalry in that industry; much of the early work on the internet was done by outsiders such as the U.S. Defense Department (ARPANET) and universities working with the federal government. The attack wasn't caused by a new entrant into that industry (the Defense Department and universities had no intention of getting into the personal computer software business).

In many ways the internet evolved without any human intention whatsoever. Corporations put together LANs first to share expensive resources such as laser printers and then later to share data, but there was never a long range plan of connecting to some sort of world wide web. Java, the language of the net, was designed as a language to make simple devices like toasters work smarter; it was never intended to be used for programming applications.

In short, the approach of the internet could never have been detected by experts systematically monitoring existing industry forces. The old game was gone, but not because of a mere shift in the existing industry forces. The internet made it possible that future computer users might not purchase boxed software at all, but might instead run applications that only exist at remote websites using their internet browsers. It was possible the future users would never buy software, but rent it as they need it. Companies like Netscape and Sun Microsystems had stolen a march on Microsoft almost without giving the matter any thought at all.

Microsoft didn't tank because, as Bill Gates puts it, they were never as clueless as the press seemed to think. In fact, Microsoft had an internet site since 1993. Still making their products internet ready was only Microsoft's 5th or 6th priority in 1995. The asymmetric internet threat could have destroyed Microsoft if they had relied on professional strategists using environmental scanning systems to detect it. Warning of the rapidly growing importance and threat of the Internet didn't come to Microsoft by way of formalized analytical processes or strategic specialists. As Bill Gates modestly admitted, the "impetus for Microsoft's response to the Internet didn't come from me or from our other senior executives. It came from a small number of dedicated (operating) employees who saw events unfolding."

The employees in question had already begun to have bad feelings about the internet, their intuition-driven fears were the product of the day-to-day grind of running Microsoft. Steven Sinofsky, for example, was stuck at Cornell University when a snowstorm prevented him from returning to California after a recruiting trip. Thus an employee involved in a fairly mundane line activity (hiring new employees) just happened to see how the internet had become a normal part of the Cornell student's everyday life. He informally observed what Gates later began to call the "internet lifestyle." A dedicated corporate planner would not have been on a recruiting trip in the first place, but even if one had been it is unlikely that he or she would have been able to appreciate what was going on at Cornell.

Mintzberg believes businesses continue to pursue the holy Grail of formalized systems because they would rather not rely on idiosyncrasies of human intuition. Still, as the Sinofsky case demonstrates, it seems that they are not only stuck with relying on human intuition but (to some extent) on dumb luck as well…what if it hadn't snowed in Ithaca, New York?

The Sinofsky case also demonstrates the impossibility of designing an environmental scanning system capable of capturing all relevant data. How could those charged with developing Microsoft's environmental scanning system possibly have known that the habits of Cornell College students would have any relevance in trying to determine the future of the personal computer software industry?

Gates himself specifically took issue with one hallmark of environmental scanning, that of staying close to the customer. As Gates noted, staying close to the customer was one of the major recommendations in Peters and Watermans' 1982 must-read, *In Search of Excellence*. However, as Gates pointed out, several of the excellent companies mentioned in that book subsequently failed despite being very close to their customers. How, Gates asked as a case in point, could the customers of Wang Labs have been of any use in warning Wang that word processing would soon be done by software running on powerful PCs and that as a consequence the days for manufacturers of dedicated word processors (like Wang) were numbered?

If environmental scanning systems don't work, what can be done to protect firms from strategic inflection points and asymmetric attacks? Advice for dealing with each threat is given in the next two sections.

Defense Against Strategic Inflection Points

> *"Life's like a ball game. You gotta take a swing at whatever comes along before you wake up and find it's the ninth inning."*
>
> - Ann Savage (hitchhiker Vera) in *Detour*

Grove offered several pieces of advice for dealing with strategic inflection points. The first issue he addressed was how to identify them. He said that the "most important tool in identifying a particular development as a strategic inflection point is a broad and intensive debate" involving technical issues, marketing issues, and strategic repercussions. Grove makes it clear that operations people should be involved in that debate (so Mintzberg's objections would not be an issue), but he goes beyond that recommending that managers at all levels and even outsiders (customers and partners) be heard. He says that the purpose of the debate is not to find unanimity, but to get to the place where everyone in the debate understands each other's point of view. He notes that strategic inflection points are generally somewhat murky and debate makes them a little clearer.

Grove also noted the value of intuition in identifying strategic inflection points and cautioned that data may be trumped by "anecdotal observations and your instincts." Again, the necessity of line manager contributions are suggested since the opportunity for "anecdotal observation" would be severely limited in the ivory tower.

Grove's third piece of advice is aimed at management personnel (although not necessarily just line management). Grove, emphasized the emotional problems in dealing with a strategic inflection point. Indeed he says managers suffering through one see their world coming to an end and will often go through a sequence of emotions similar to those "associated with grief (i.e., denial, anger, bargaining, depression, and ultimately, acceptance)." Unfortunately some managers may be too vested in the status quo to be able to get to the acceptance state. The advice is that these managers (their loyalty to the organization not withstanding) should be replaced.

Grove's main concern with strategic inflection points (as the last paragraph indicates) is that management often simply refuses to act. Unfortunately they may think they are acting; they may talk the talk, but not realize they are not walking the walk. He says that "strategic dissonance" is where a company falls into the trap of "saying one thing and doing another…" His fourth suggestion is therefore that management loosen the level of control over lower managers who may be more inclined to try something new if given the freedom to act; that experimentation at lower levels might be a remedy to this inaction at higher levels.

Grove's fifth recommendation is to respond to a strategic inflection point as soon as possible. He warns that almost no matter what a company's intentions are they are unlikely to react as soon as they should. He confessed, "I have never made a tough change, whether it involved resource shifts or personnel moves, that I haven't wished I had made a year or so earlier." Grove also offers advice on what to do in the phases after environmental scanning (such as putting together a new vision, etc.), but that is beyond the scope of this paper.

The next set of recommendations deal with the more difficult problem of the asymmetric attack. As will be seen, the recommendations would probably be considerably harder to put into practice.

Defense Against Asymmetric Attacks

The U.S. Army Strategic Studies Institute suggests five defenses against asymmetric attacks: maximize conceptual and organizational adaptability, focused intelligence, minimize vulnerability, full dimensional precision, and integrated homeland security. The first three of the five defenses would seem to be workable in a business environment. Those three lead to several recommendations which will be explained in the following paragraphs.

If we can't anticipate an asymmetric attack we might at least be able to react to one when it occurs. Maximizing conceptual and organizational adaptability means making sure the organization develops the habit of innovating and thinking creatively.

This does not mean putting the artists in charge; the Strategic Studies Institute states flatly that "iconoclasts and nonconformists should not rule the military" but "should (nevertheless) be valued, preserved, and heard."

This aspect of the SSI's thinking is in accord with Mintzberg. While the artists and "staff weenies" (as the army calls them) may come up with some very creative ideas, they lack the experience-generated intuition needed to synthesize information. The artists can, however, help train line people to think creatively.

The SSI suggests that the creative thinking of line managers can be developed by exercise, which in the case of the military means wargames. But conventional wargames present only standard threats so the SSI recommends that the military occasionally conducts wargames which present asymmetric threats. The artist's creativity could be harnessed to develop truly challenging threats.

Wargames should not be confused with analytical technique of scenario development as recommended in the strategy literature (such as in Thompson and Strickland). Scenarios are different from wargames for a number of reasons. First, those who develop scenarios hope to develop one which will actually match what the future turns out to be. The SSI does not recommend that wargame designers even try to present a likely asymmetric attack scenario since that would be impossible give that there is no such thing as a "likely" asymmetric threat.

The purpose of the unconventional wargame isn't to learn to deal with the particular situation presented, but rather to learn to deal with the unexpected in general. For example, the creative thinking that might have been exercised in training on a wargame involving an asymmetric small pox attack on Chicago might have helped strategists react better to the September 11 attack in New York. It is, of course, entirely possible that such wargames were played out; certainly the New York City Mayor's Office and federal officials did seem to react very effectively to the disaster.

The second difference between scenarios and unconventional wargames is that scenarios are developed by professional strategists (the artists) for their own use in developing strategy. Unconventional wargames, may be developed by professional strategists, but their purpose it to exercise the creative thinking of operations personnel.

Mintzberg was especially critical of scenario building. He asked how anyone could possibly know how many scenarios would be enough to cover all important contingencies. He also asked what is to do after developing the scenarios: are businesses to prepare for just one, for all of them, etc.? Neither of these criticisms apply to unconventional wargames since they are not designed with the intention to cover all possible contingencies (or even a likely one for that matter).

SSI has one piece of additional advice with respect to wargames and that is to make sure the "red team" (the bad guys) has the resources it needs to give the "blue team" (the good guys) a run for their money. In a business wargame there may be no actual red team, but the simulated threat should be as unexpected and serious as possible. A wargame scenario at Intel, for example, might have involved the case where Texas Instruments had just developed a microprocessor orders of magnitude faster than anything then on the market.

The SSI suggests that conceptual and organizational adaptability can be enhanced by more than just wargames. They also recommend "making modularity a central criterion in the force development process." This means that the Army should acquire people and systems that will “plug-and-play” so they can rapidly build task-specific organizations from the ground up. The SSI uses the term “agility” to describe this capability. Agility is the same concept that has been widely used in the business literature since it was popularized by Goldman et. al. in 1995.

Huffman and Amundson (1995) give advice for judging an organization’s agility. They provide metrics for evaluating the plug-compatibity of a business organization’s units. Specifically, the metrics are for evaluating the way those units are linked together and the subsequent performance of the linked organization.

The SSI’s second recommended defense against asymmetric attacks is “focused intelligence.” The SSI notes that “U.S. intelligence efforts need to be at least partially refocused on nontraditional threats, including asymmetric ones.” This may sound like environmental scanning, and to some extent that is true. But this advice goes beyond the usual environmental scanning because what is being recommended is that the military look in some places where it hasn’t been looking and to “think differently” about intelligence collection. The SSI notes the conventional wisdom that more human intelligence (more spies) is needed, but they recommend thinking even more broadly about intelligence (perhaps, for example, using very unusual technology such as robots to collect intelligence data).

Still under the heading of “focused intelligence” the SSI recommends more synthesis (as opposed to analysis); they say that synthesis can be enhanced by breaking down barriers between intelligence agencies. There was certainly a lot of environmental scanning and analysis going on at the FBI before the September 11 attacks on the World Trade Center and Pentagon, but what was sadly lacking was a synthesized picture of the impending attack that might have been possible had the barriers both within the FBI and between the FBI and other intelligence agencies been torn down. Just as Mintzberg would have predicted, analytically inclined experts at the FBI Headquarters in Washington would be too removed from their own field agents and the day-to-day grind necessary to develop the proper intuition. The existence of a barriers within the FBI was apparent in FBI Headquarter’s dismissals of many requests from field agents; either the field agents were asking for too much or FBI Headquarters was denying too much, but both parts of that organization were obviously not on the same page.

Frederick Forsyth, successful novelist and former soldier-of-fortune, agreed with the last two recommendations in his December 12, 2002 opinion piece in *The Wall Street Journal.* He also stressed that focused intelligence and synthesis are needed. As for focused intelligence he called for an increase in counterintelligence which he said “is based on knowing the enemy, who he is, where he is, what he plans and when.” According to Forsyth, counterintelligence necessarily means putting your people in the enemies organization…this would certainly be looking in a new place but would also probably be taking things a little to far in the business world.

As for synthesis, Forsyth noted that, “What went wrong before Sept. 11 was not that nobody knew anything; it was that various agencies knew (or suspected) bits of something looming but could not put the jigsaw together alone, and had no in-place mechanism for cross-indexing what they had.” Forsyth thought that a model for synthesis might be the British Joint Intelligence Committee where top people from their equivalent of the CIA, FBI, and NSA can all meet at one table. Mintzberg might agree as long as the representatives include some operations people. Otherwise Forsyth might have been closer to the correct model in his novel *The Day of the Jackal* where top government leaders did meet around a table, but their meetings included a lowly police officer who in the end was the one who was able to stop the Jackal.

Bill Gates came close to *The Day of the Jackal* model with his recommendations concerning corporate CIOs. He noted that these operations-oriented individuals are often left out of corporate level strategy sessions (even those involving information systems strategy). Gates recommends that corporate CIOs be in on corporate strategy meetings and sign off corporate goals for information systems (both the tasks to be done as well as their priority).

Gates also noted that Microsoft has a biannual "Think Week" which is dedicated to the type of synthesis the SSI recommends. During Think Week, Gates sets aside "all other issues to concentrate on the most difficult technical and business problems facing the company." From where do the ideas for the Think Weeks come? Gates describes the corporate thinking aloud that goes on at Microsoft when someone begins a email chain. Email chains at Microsoft flesh out strategic issues of concern; anyone who has anything to say jumps into these discussions. Once the email chains get long enough, once there are enough issues and recommendations to consider, retreats (or Think Weeks) are planned to produce decisions.

The SSI's third recommended defense against asymmetric attacks is to reduce the Army's vulnerability. This rule boils down to two pieces of advice: first the army should keep moving (moving targets are harder to hit) and second they should not depend on one of anything (dependency equals vulnerability). In business "keep moving" might translate to pursuing a policy of adequately funding both R&D and continuous improvement.

When the SSI talks about not relying on one of anything, they mean more than just one material thing such as one weapon; they also mean one method, one system, etc. For example, the SSI is concerned that the U.S. military is too dependent on information superiority or digital technology. When the fog of war temporarily robbed the Army of its high-tech information superiority in Somalia; soldiers had trouble quickly finding their way to two Blackhawk helicopter crash sites. Every minute of delay meant they had to fight more and more enemy soldiers when they finally did arrive. The soldiers clearly could have benefited from a lower-tech backup method for navigation.

The business ramifications relying on one of something are almost very serious. In the past Intel relied heavily on the memory chip business. Today Intel relies heavily both the microprocessor business (which means they rely on the P.C. business), and on integrated circuit technology. Both vulnerabilities leave them open to attack as deadly as the one that ruined their memory business.

Conclusions

"Hey, I like this. Early nothing."

- Gloria Grahame (gangster moll Debby Marsh) about a fleabag hotel room in *The Big Heat*

The world and business are both a lot more dangerous than we would like them to be. Managers would like the academe to offer them a way out and the academe would like to provide it. Unfortunately, false security is worse than fear. Environmental scanning systems are false security. They are not capable of detecting asymmetric threats and, although they can detect strategic inflection points, management isn't likely to heed their warning.

Some advice has been given here for dealing with both asymmetric threats and strategic inflection points, but nothing that has been offered here is intended to make managers feel secure. While a lot has been said about the value of the intuition of operations personnel, the manager (in the end) will also need a little luck and anyone who offers that should probably be searched before they leave the building.

References

Forsyth, Frederick. "Your Spies Could be More Like Our Spies" *The Wall Street Journal,* December 12, 2002, page A18 column 5.

Gates, William. *Business @ the Speed of Thought*, New York, NY: Warner Books, 1999.

Goldman, Steven L., Roger N. Nagel and Kenneth Preiss. *Agile Competitors and Virtual Organizations: Strategies for Enriching the Customer*, New York, NY: Van Nostrand Reinhold, 1995.

Grove, Andrew S. *Only the Paranoid Survive: How to Exploit the Crisis Points that Challenge Every Company and Career,* New York, NY: Doubleday, 1996.

Huffman, Brian J. and Susan D. Amundson, "Plug-Compatible Groups: Theory and Vision of a Structure for Manufacturing Organizations" *Proceedings of the 26th Annual Meeting of the Decision Sciences Institute,* November 20-22, 1996.

Peters, Thomas J. and Robert H. Waterman, Jr. *In Search of Excellence: Lessons from America's Best-Run Companies*, New York, NY: Warner Books, 1982.

Thompson, Arthur A. and A. J. Strickland III, *Strategic Management: Concepts and Cases,* Boston, MA: Irwin McGraw-Hill, 1998.