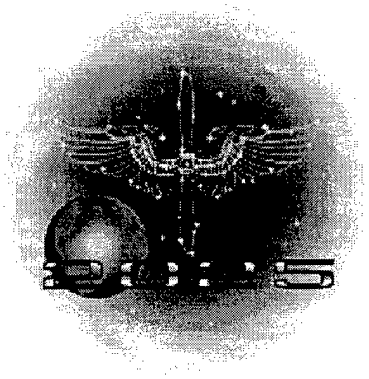
Hit'em Where It Hurts:
Strategic Attack in 2025



A Research Paper
Presented To

Air Force *2025*

by

Lt Col Jeffrey E. Thieret
Maj Steven J. DePalmer
Maj Frederick I. Guendel, Jr.
Maj Michael A. Silver

August 1996

Disclaimer

2025 is a study designed to comply with a directive from the chief of staff of the Air Force to examine the concepts, capabilities, and technologies the United States will require to remain the dominant air and space force in the future. Presented on 17 June 1996, this report was produced in the Department of Defense school environment of academic freedom and in the interest of advancing concepts related to national defense. The views expressed in this report are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States government.

This report contains fictional representations of future situations/scenarios. Any similarities to real people or events, other than those specifically cited, are unintentional and are for purposes of illustration only.

This publication has been reviewed by security and policy review authorities, is unclassified, and is cleared for public release.

Contents

Executive Summary

In the year 2025, advances in technology should allow air and space assets to affect an adversary anytime, anywhere. The ultimate goal of strategic attack is to conduct operations "to a point where the enemy no longer retains the ability or will to wage war or carry out aggressive activity."[1] Employing a "hit 'em where it hurts" philosophy, 2025 strategic attack operations run the gamut from traditional, highly destructive, force-on-force encounters to much less invasive, but very effective, computer-based warfare.

The diverse nature of potential adversaries, and the vast amount of information pertaining to them, requires an integrated approach to protecting American and allied security interests. Technological advances will enable all levels of leadership to successfully deal with the vast volumes of information in ways not envisioned or realized in the past. These advances will make it possible to accurately determine and engage an adversary's Locus of Values (LOV). The LOV is that which an adversary holds dear, and which if influenced or threatened would affect the enemy's ability or will to carry out covert or overt aggression against the United States.

LOVs are hard or soft. Hard LOVs are physical things: militaries, weapons of mass destruction, or industries. Soft LOVs are intangible things: Systems, knowledge, or ways of thinking. LOVs are engaged immediately or never, lethally or nonlethally, directly or indirectly. Each strategic situation is unique, yet in every case, the "force" applied against an LOV focuses on a strategic effect.

The key elements of strategic attack in 2025 are system analysis, target acquisition, target engagement, and feedback. Each phase is integrated and connected in virtual real time with the others through an organic integrated system directed to, and interpreted by, human decision makers.

Notes

[1] Department of the Air Force, *Air Force Doctrine Document 1, Air Force Basic Doctrine* (draft) (Langley AFB, Va.: USAF Doctrine Center, 15 August 1995), 13.

Chapter 1

Introduction

Strategic attack in the 2025 program is both unchanged from what it has been throughout human history and yet radically different. How can this duality be true? The truth is found in the ends and means of strategic attack.

Across time, the objective of strategic attack has been to conduct operations that would have a war-winning effect on an adversary. We need look no further than proposed Air Force doctrine, which asserts that the goal of strategic attack is to conduct operations "to a point where the enemy no longer retains the ability or will to wage war or carry out aggressive activity."[1] In other words, we are doing things that will affect the entire war, not just a particular target, battle, or campaign. Therefore, it is the end result of strategic attack that has not changed.

The part of strategic attack that has changed involves the means. The methods by which attacks are planned and conducted to produce strategic effects will be very different in 30 years. The leaping advance of technology, different ways of organizing these technologies, and evolving military doctrine guarantee that the means will change. Clearly, strategic attack is not about weapons—any weapon can be strategic if it affects the adversary's ability or will to wage war. Furthermore, the same weapon can be tactical, operational, or strategic, depending on its use and how it affects the enemy.

The key to strategic effect is the opponent's values. Every adversary is unique; therefore, every strategic attack will be different. This idea has been handed down through generations of warriors as the concept of a center of gravity (COG).[2] The term *COG* created a good image in an age of Lapacian determinism, where machinery was the model; however, in 2025 the view is more organic, so the COG

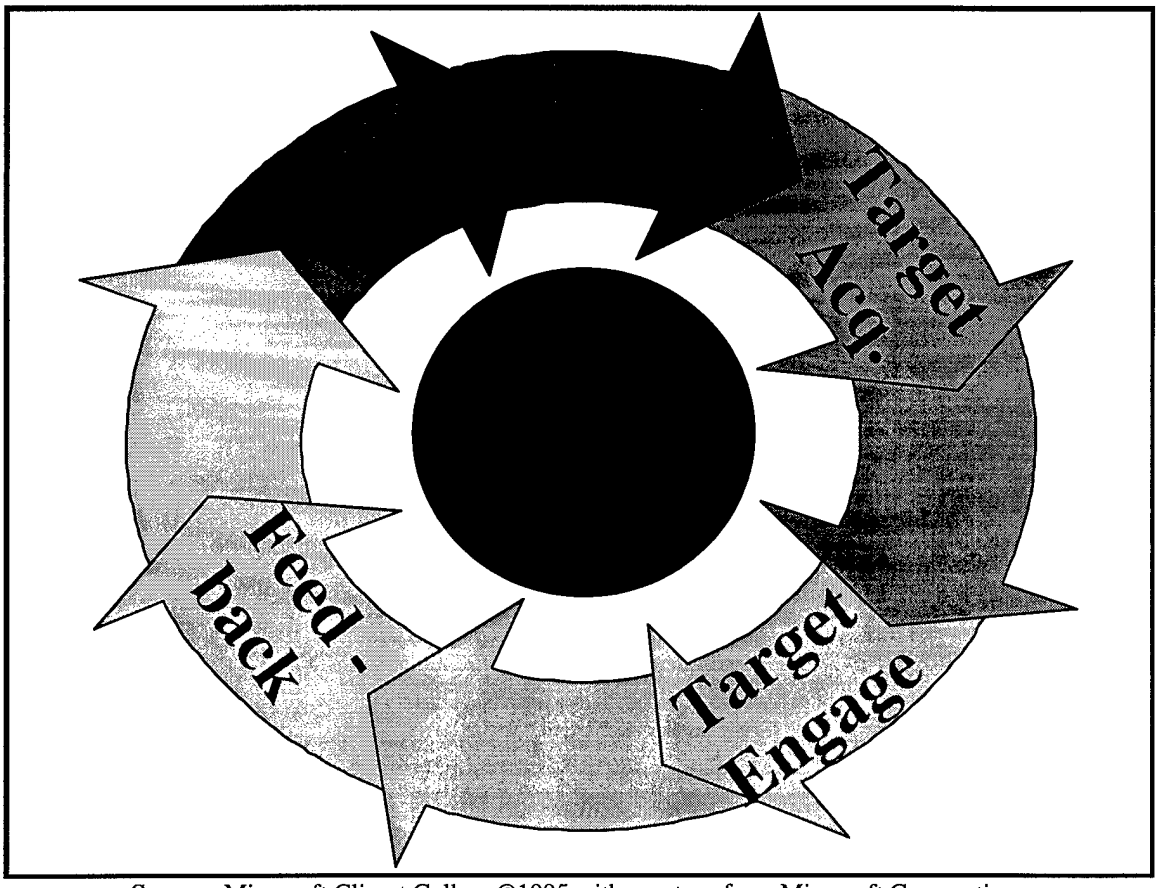
concept loses some of its usefulness. A more descriptive term is LOV: that which is held dear and which, if influenced or threatened would affect the enemy's ability or will to wage war or carry out aggressive activity.[3]

Armed with the term *LOV*, we turn to the wave metaphor of Alvin and Hiedi Toffler for a framework in which to conduct strategic thinking. The Tofflers' paradigm asserts that human societies are evolving upward in waves, rather than in a constant climb. The societal waves are split into three segments, based upon what drives the entity's economy: agriculture, industry, or information. Further, the values of each wave society differ from those which another wave holds dear.[4] The world in 2025 will contain societies rooted in each wave.

The Toffler model is useful to the warrior because it can be applied to a diverse range of potential adversaries. By using the wave model to ascertain the dominate societal focus of an adversary, one can gain insight into critical LOVs. With LOVs accurately determined, the samurai of 2025 can prosecute an effective strategic attack.

The Toffler wave model provides a point of departure for planning attacks.[5] It suggests that: (1) first wave adversaries are best dealt with by targeting individual leaders or territory; (2) second wave opponents will be threatened by destruction of armies or industry, and (3) third wave enemies focus on idea-centered technologies or economies.[6]

The wave model helps us think about what to attack to achieve strategic effect, which is but one part of the process. Knowing the correct LOVs must be combined with acquiring and engaging them, and then determining if the attack was effective. This organic strategic attack process produces war-winning effects against an adversary. Figure 1-1 illustrates four key elements of strategic attack: system analysis, target acquisition, target engagement, and feedback.



Source: Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

Figure 1-1. Strategic Attack Process

Information links the above four elements of strategic attack. Information revolves primarily around the adversary's LOV, which eventually becomes strategic "targets" comprised of many dimensions. LOVs are either hard or soft. Hard LOVs are physical things: militaries, weapons of mass destruction, or industries. Soft LOVs are intangible things: systems, knowledge, or ways of thinking.[7] Both are engaged immediately or never, lethally or nonlethally, directly or indirectly. Each case is different, yet in every case the force applied is aimed at strategic effect.

Notes

[1] Department of the Air Force, *Air Force Doctrine Document 1, Air Force Basic Doctrine* (draft) (Langley AFB, Va.: USAF Doctrine Center, 15 August 1995), 13.

Illustrations

Tables

Chapter 2

Required Capabilities

Strategic attack in 2025 requires certain capabilities. Some capabilities will evolve from current organizational doctrine and technology. Other capabilities require revolutionary developments, much different from current tools of strategic attack. The capabilities required for each element of strategic attack are categorized as shown in Table 2-1.

Table 1

Strategic Attack Requirements for 2025

Strategic Attack Element	Required Capability
System Analysis	Knowing the LOV
Target Acquisition	Locating the LOV
Target Engagement	Affecting the LOV
Feedback	Determining results

System Analysis

In his pamphlet *10 Propositions Regarding Airpower*, Col Phillip Meilinger suggests that "In essence, Airpower is targeting, targeting is intelligence, and intelligence is analyzing the effects of air operations."[1] Knowing what to attack to achieve the desired effect is the critical element. Further, what to target varies greatly between adversaries. The LOV for a textbook second wave nation may be its industrial web. For a nation possessing a small military capability, yet wielding tremendous informational and economic might, the LOV may be their information infrastructure. For nonstate actors such as terrorist organizations, drug cartels,

or organized crime syndicates, the LOV may be their leadership. In short, knowledge acquisition is particularly important in strategic attack because the aim is to impact across the whole of an adversary from highly focused inputs.

Knowing "what" to attack has always been difficult, and it will become harder in 2025 for a number of reasons. The first concern involves the growing number of actors. A burgeoning number of sovereign states, emerging transnational groups, multinational corporations, and other organizations will influence US policy. Next, add increased access to previous "close hold" information through the explosion of media, the Internet, and population migration. And finally, stir in a world political dynamic that is much more fluid than during the cold war. Because of all these challenges, the system analysis problem becomes incomprehensible to the unaided human decision maker.

The human decision maker's ability to determine strategic LOVs in 2025 will come from a combination of technologies. These include exploiting national and global databases, employing artificial intelligence (AI) technologies to turn that data into usable information, and using increased computational capacity to run the AI programs in a near-real-time fashion.

Exploiting data 30 years hence will certainly remain a daunting task. The USAF Scientific Advisory Board (SAB) addresses this problem in their *New World Vistas* study: "Much of the information which is needed to construct the global picture exists today in computers somewhere. The problems of the next decade are to identify the relevant databases, to devise methods for collecting, analyzing, and correlating them, and to construct the needed communication and distribution architectures."[2] Therefore, a critical enabling capability to conduct strategic attack in 2025 is an ability to exploit all relevant sources of existing and emerging data.

Turning the acquired data into useful information for strategic decisions is the task of AI technologies. AI is a multidisciplinary field that aims to develop device technologies capable of solving problems in a manner similar to that of a human being. AI permits a computer to constantly comb vast amounts of data for useful kernels of seemingly unrelated data, process them into information, and then deliver that information to decision makers in a timely manner. Advanced AI is required to correlate the mountain of unorganized data located throughout the information domain.[3]

AI technology employs sophisticated computer programs. By its nature, AI requires large amounts of computational ability and storage capacity. Current hardware meets the needs of today's AI applications; however, by 2025 AI applications will require faster processors and much larger data storage capacities.

Target Acquisition

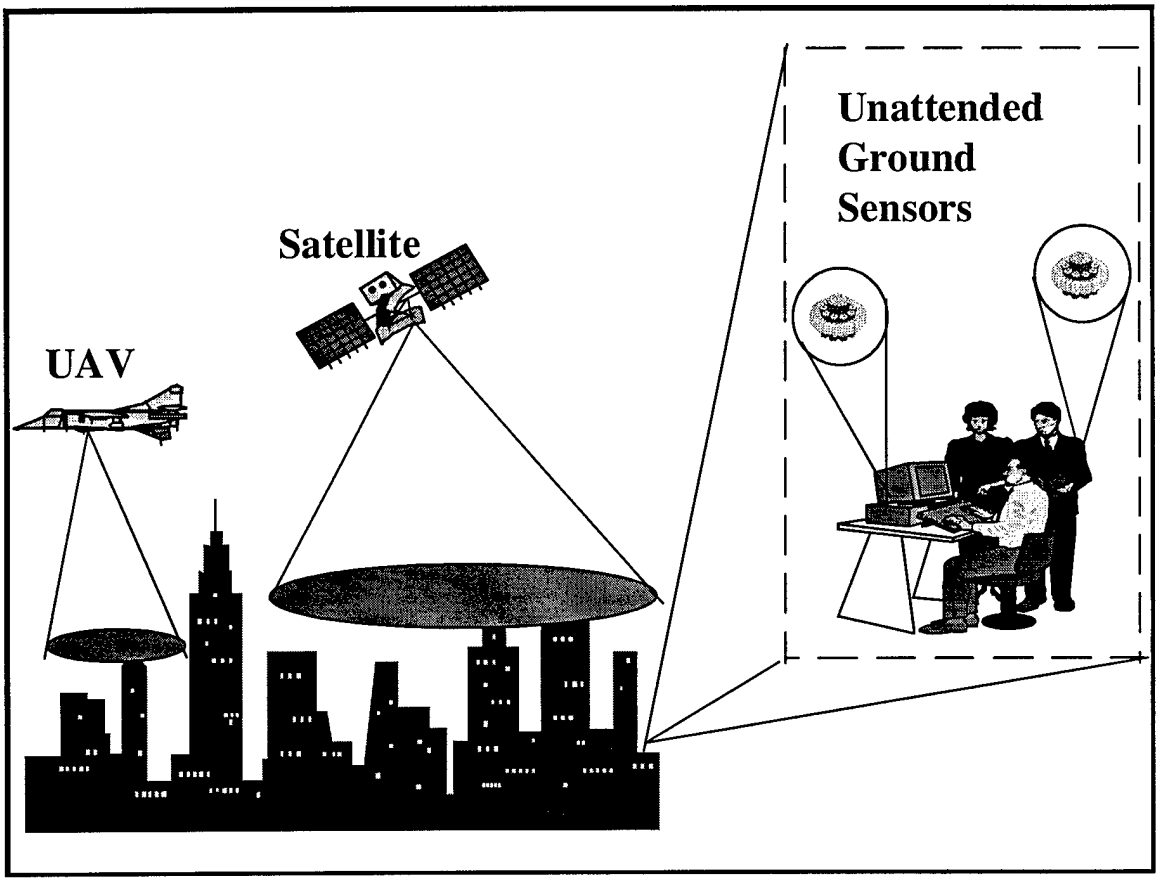
As mentioned previously, the AI system requires a cumulative database to help decision makers determine the possible LOVs of an adversary.[4] A portion of that AI database originates from the target acquisition system. Target acquisition involves the continuous collection of data for analysis and use by the AI network. A collection of sensors search for different types of signatures common to LOVs. This data is transmitted in virtual real time to the AI database to be analyzed and applied to the strategic attack process.

The target acquisition system does not simply push data to the AI network; it also must pull information from the network. Pulling information from the AI network narrows the search pattern for the sensor platforms and reduces the time required to locate specific targets. For example, the AI network may determine that an LOV for a certain adversary involves the capability to produce and employ chemical weapons. The target acquisition system can orient itself to search more efficiently by pulling from the AI network details such as the probable chemical composition and size of strategic production facilities, about the LOV. Once the LOV is located, the sensor platforms periodically revisit the region to detect any changes in activity.

In order to locate specific LOVs, the target acquisition system requires novel sensors that essentially can see, hear, smell, taste, and touch. Current target acquisition systems for strategic attack depend heavily on sensors that only provide image data from the infrared and visual spectrums. Having different types of sensors in 2025 provides complementary data for the AI network to analyze and helps detect an adversary's LOVs.

The platforms supporting the sensor array vary, depending on the sensor's capability. As shown in figure 2-1, space and airborne platforms, including stealthy unmanned aerial vehicles (UAVs), can operate jointly to provide the AI network continuous coverage of a specific region or land mass. Unattended ground

sensors (UGS) rely on their minute size to avoid detection by an adversary. In 2025, sensors the diameter of a human hair will allow continuous, stealthy, on-site collection, providing the AI network the critical data necessary for making decisions concerning strategic attack.[5]



Source: Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

Figure 2-1. Sensor Platforms

The final requirement for target acquisition in 2025 involves the necessity for sensor data to be transmitted instantaneously to the AI database. Sensor platforms such as satellites and UAVs can transmit data directly to relay stations on the ground or in orbit. Tiny unattended ground sensors depend on an external source to amplify sensor signals. The end result is complementary data from different sensor arrays delivered simultaneously to the AI network for analysis and application in the strategic attack process.

Target Engagement

In 1943, according to McKitrick et al in *The Revolution in Military Affairs*, the U.S. Eighth Air Force prosecuted only 50 strategic targets during the entire year. In comparison, during the first 24 hours of Desert Storm, the combined air forces prosecuted 150 strategic targets—a thousand-fold increase over 1943 capabilities.[6]

In the year 2025, air and space power must make a similar leap in capability to ensure that the US maintains the advantage against its potential enemies. This will be accomplished through capabilities that affect LOVs in a very diverse manner. The system analysis and target acquisition processes provide the details of how to engage each LOV. These details can be characterized by the three boundaries depicted in figure 2-2. The first boundary ranges from lethal to nonlethal force. The second boundary involves the use of either direct or indirect means. The last boundary indicates that the time to engage an LOV will range from immediately to never.

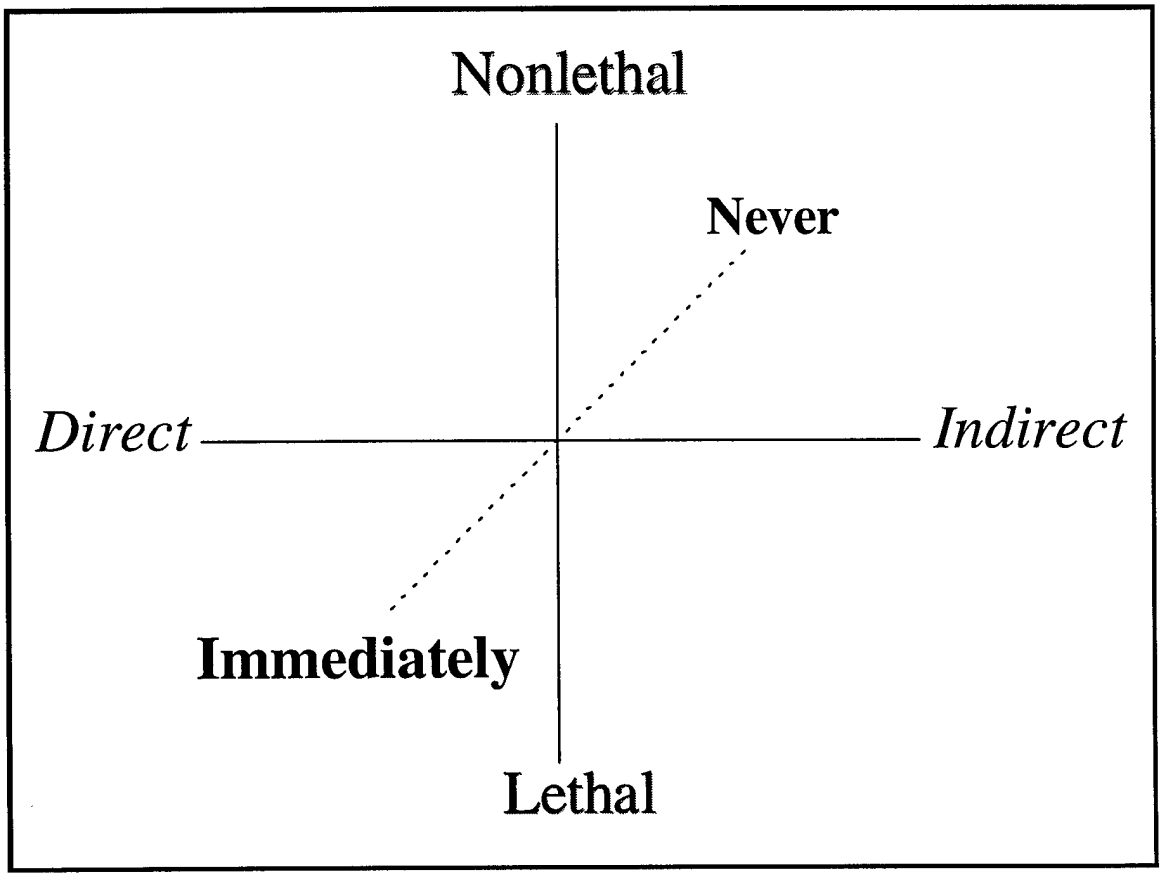


Figure 2-2. LOV Engagement Spectrum

The application of airpower has traditionally been accomplished by directly applying lethal force. However, many cases in the future will call for nonlethal force, especially when engaging another advanced "post-industrial" society. For example, against a third wave adversary we might attempt to disrupt, dominate, and then reorder an enemy's decision cycle.[7]

Although the Gulf War demonstrated that airpower can deliver direct, lethal force against a target set, there remains much room for improvement. As military force structures continue to downsize, we will lean towards systems capable of affecting multiple LOVs per mission. Instead of an F-117 flying over Baghdad to drop two precision guided munitions (PGM), it is more cost-effective to deliver dozens of PGM-type munitions on the same mission. In 2025, this capability allows a single mission to have the same results as a squadron of F-117s.

An organic, multiple engagement capability increases the application of air and space power throughout the enemy's strategic system with such great speed and momentum that hyperwar results. The simultaneous engagement of LOVs makes an adversary's recovery difficult because the remaining energy available to the system is inadequate to restore it to full capacity.[8]

The time to engage a strategic LOV can range from "immediate" to "never." An example of "never" is making a conscious decision not to attack an enemy's head of state, as in the case of Iraq's Saddam Hussein. Another example is the "Ultra" intercepts of Nazi war plans during World War II. Indeed, Churchill had to make numerous painful decisions not to defend Allied assets he knew were going to be attacked for fear of alerting the Germans to prior Allied knowledge of their plans.[9] On the other hand, we need the capability to engage some LOVs "immediately." An example is a convoy of NBC weapons discovered less than a mile away from a hardened storage facility deep inside a mountain. The US might have less than one minute to react and destroy these weapons before the engagement opportunity disappears.

The key to successful target engagement is having the air and space power to execute target engagements in terms of lethal or nonlethal force, direct or indirect means, and at the correct time. This will be accomplished by a combination of improvements in weapons and strategic attack platforms.

Feedback

Following a target engagement, the AI network requires near-real-time postattack data to determine subsequent courses of action. Having an instant feedback capability shortens the operational timeline required for strategic attack in 2025. The same sensors used for target acquisition provide the necessary feedback data to the AI network. The data from different sensors is collected and then quickly fused into accurate mission evaluation results by the AI network. This feedback process answers the question as to the outcome of the strategic attack: To what degree did the mission succeed or fail, and did any positive or negative side effects occur that require further action?[10]

Notes

[1] Col Phillip Meilinger, *10 Propositions Regarding Airpower,* (Air Force History and Museums Program, 1995), 1.

[2] USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century,* summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 25.

[3] Ibid., 38-44.

[4] The proposed system is designed provide suggested LOVs to human decision makers, along with the thought processes behind their selection. The human will then make engagement decisions.

[5] Gary Stix, "Micron Machinations," *Scientific American,* November 1992, 107.

[6] Jeffrey McKitrick et al., "The Revolution in Military Affairs" in Barry R. Schneider and Lawrence E. Grinter, eds., *Battlefield of the Future* (Maxwell AFB, Ala.: Air University Press, 1995), 78.

[7] Barry R. Schneider and Lawrence E. Grinter. *Battlefield of the Future* (Maxwell AFB, Ala.: Air University Press, 1995), 149.

[8] Col Richard Szafranski, "Parallel War and Hyperwar: Is Every Want a Weakness" in Barry R. Schneider and Lawrence E. Grinter, eds., *Battlefield of the Future* (Maxwell AFB, Ala.: Air University Press, 1995), 128.

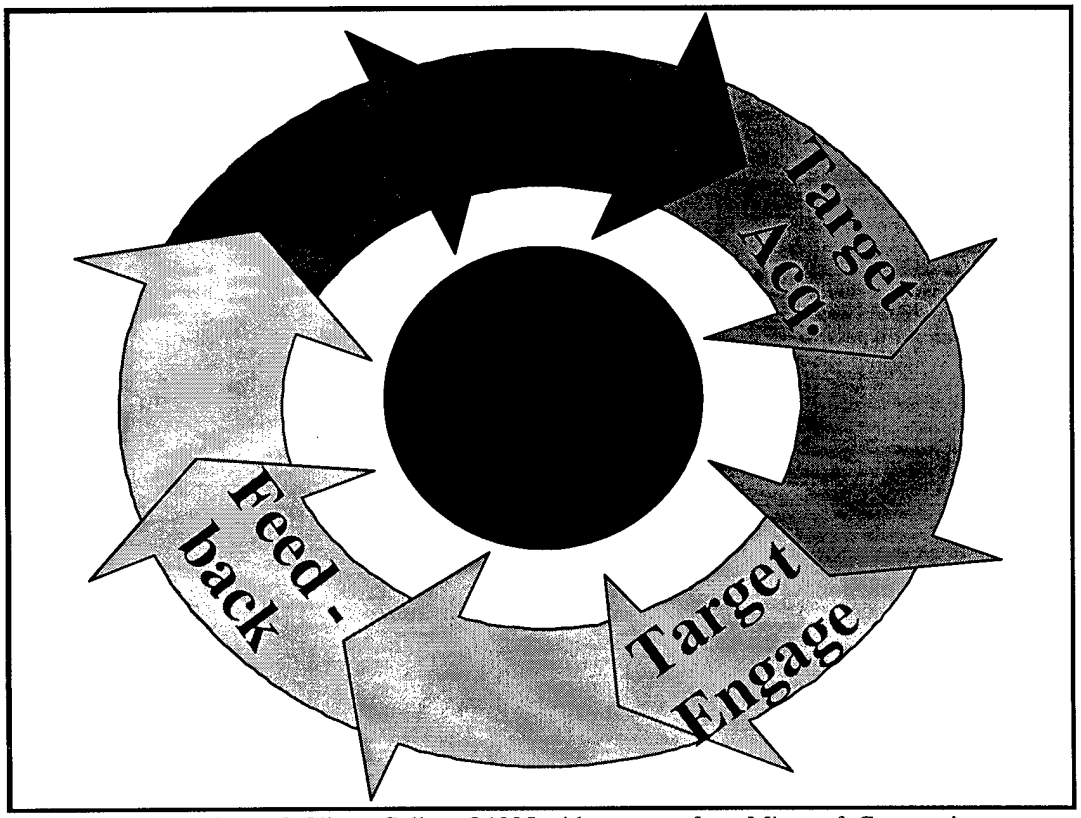
[9] Schneider and Grinter, 150.

[10] The measure of success that the system would be reporting to human decision makers would focus on the desired effect on enemy decision makers.

Chapter 3

Strategic Attack Systems Description

The process required to conduct strategic attack in 2025 uses a "system of systems," with each subsystem solving one particular part of the attack problem (fig. 3-1). The process is organic, in the sense that all of the parts are interlinked and interactive, each receiving and delivering input to the others. It provides targeting information containing the LOVs upon which the US should act, whether they are hard or soft, should be acted on now or never, lethally or nonlethally, and directly or indirectly.

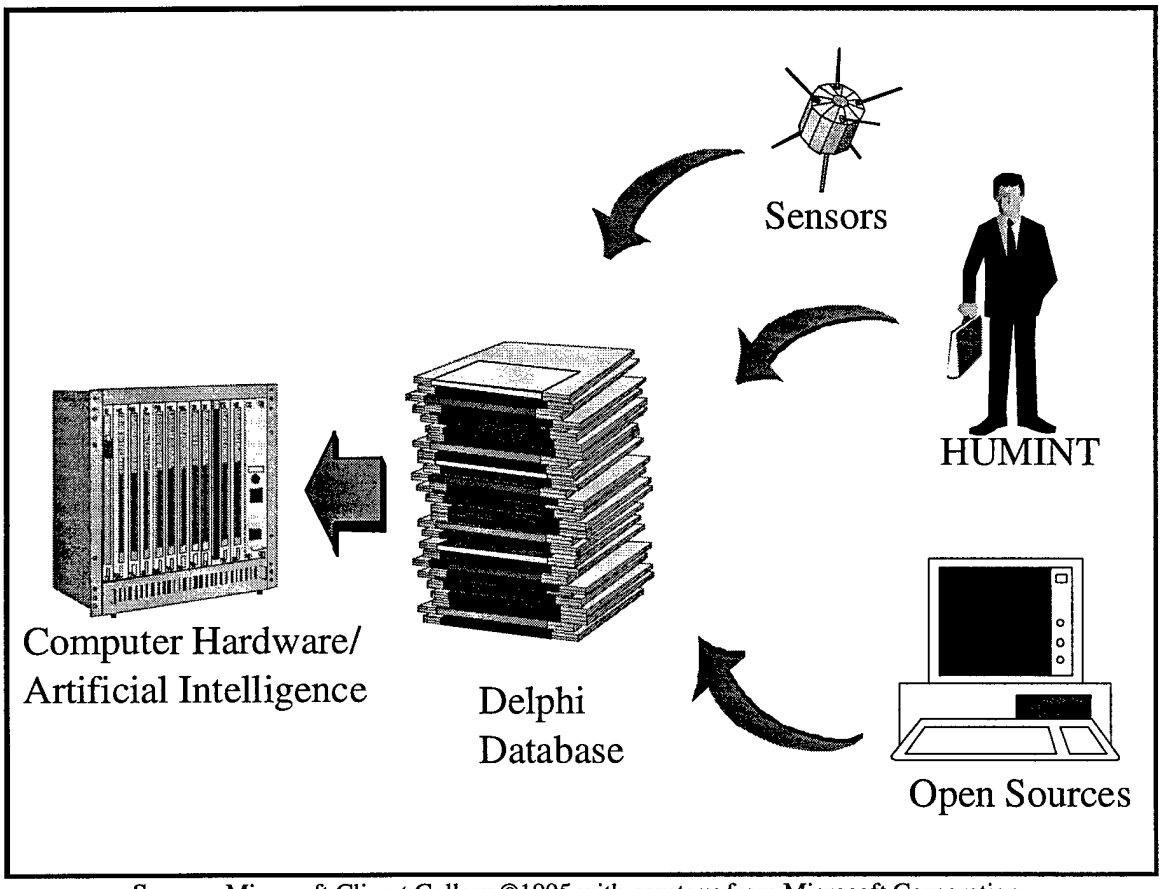


Source: Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

Figure 3-1. Strategic Attack Process

System Analysis System

A component of the strategic attack model is the system analysis system, this which will operate for decision makers in 2025. It will be composed of a pervasive, distributed, relational database; a blackboard artificial intelligence architecture; and a massively parallel, distributed computing capability. The system analysis system, shown in figure 3-2, functions to provide the decision makers with the knowledge that they need to direct strategic attack.

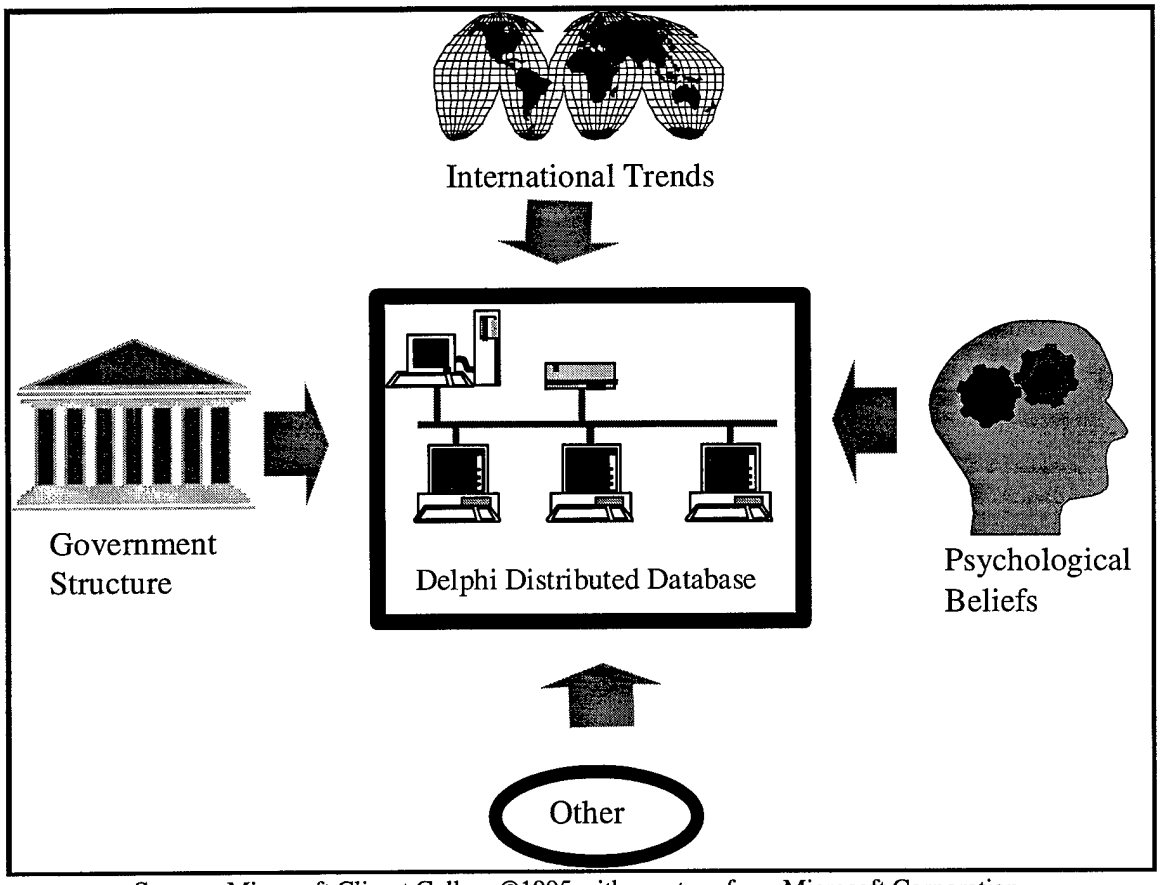


Source: Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

Figure 3-2. The System Analysis System

The 2025 system analysis system relies on a pervasive, distributed, and relational database.[1] The data comes from all sources, spanning the spectrum from state of the art sensors collecting information in virtual real time, to archives on ancient history and culture. Because the database is so pervasive and distributed, it functions as a database of databases, with the primary users of each segment maintaining their separate parts. Its decentralized, and partitioned structure permits data to be added or altered as future experience shows is

necessary.[2] A depiction of this type of database arrangement is shown in figure 3-3. In this diagram, four widely separated databases combine to form the Delphi database for the strategic problem or problems that the system is working. The actual titles of the databases in figure 3-3 are notional. The important points to note are that the individual databases originate from virtually anywhere and are tied together by a network to comprise the Delphi system for solving a particular problem. A different set of variables would result in a different database combination.



Source: Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

Figure 3-3. Delphi Database

The technology to facilitate this database will develop at varying rates, so the structure of the database allows the components to be incorporated as they emerge. Electronic data storage and access rates are advancing at a great pace. A recent study suggests that likely advances in optical disk technology and applications of "parallelism" hold the potential for significant increases in storage capacity.[3] Broadband fiber optic networking technologies that allow for the distributed nature of the system are advancing and will continue to improve volume and speed of data transfer. The USAF SAB postulates that ultra-high-speed

broadband commercial backbone networks will be widely available by 2005. This infrastructure essentially gives infinite bandwidth to all users, therefore minimizing networks as a limiting factor for the database system.[4]

Access to diverse amounts of information could be a problem. As the value of information grows in the world economy, many distributed databases may become proprietary, denying the Department of Defense (DOD) access. The networked and distributed nature of the Delphi database requires the ability to secure the sensitive parts of it.

The Delphi database could, of course, be countered in a number of ways. The potential opponents of the US could shield the data that we desire. They could prevent our sensors from observing sensitive physical targets, or they could attempt to camouflage or obscure them. Opponents could close their societies, preventing us from collecting information concerning who their leaders are and how they think. Additionally, they could physically attack the data storage or transmission infrastructure or corrupt the data contained in the system. The best counter for attempts to prevent our data collection is a redundant and complementary collection system—many different types of sources. Possible countermeasures against data corruption include comprehensive physical security and defensive information warfare measures.

Artificial Intelligence

AI involves programming a computer to solve problems that normally only people can handle. In 2025 AI provides the help that humans need to make strategic attack decisions. The role of AI is to constantly process the data stored in, and streaming through, the Delphi database. The ultimate goal is to use AI to determine the best way for the US to conduct strategic attack against an emerging opponent. A number of different AI approaches exist, a partial list of them includes expert systems, CBR, and neural networks.

Expert systems turn the knowledge of a human expert into a computer program, and through an "if. . .then. . .else" process, applies that codified knowledge to similar, future problems. They cannot extend that knowledge outside the expert's field.[5] CBR is a technique that suggests actions by recognizing similarities between current problems and previously solved occurrences. Because CBR focuses on past problem resolutions rather than the current problem, it is quickly and easily implemented. To the point that new problems differ from those of the past, however, CBR has less value.[6] The third AI approach involves

neural networks. They employ real-world ambiguous data points to determine a relationship, apply the relationship to make decisions, and constantly review the derived relationship to learn and improve the decision making process. Neural networks require, neither a human expert's knowledge nor past occurrences of the problem in order to function. Further, they can make constantly improving predictive decisions.[7]

The architecture of the AI portion of the system analysis process involves a modified blackboard expert as shown in figure 3-4. A blackboard system is a hybrid expert system comprised of a collection of independent components called "blackboard," "knowledge modules," and "control module."

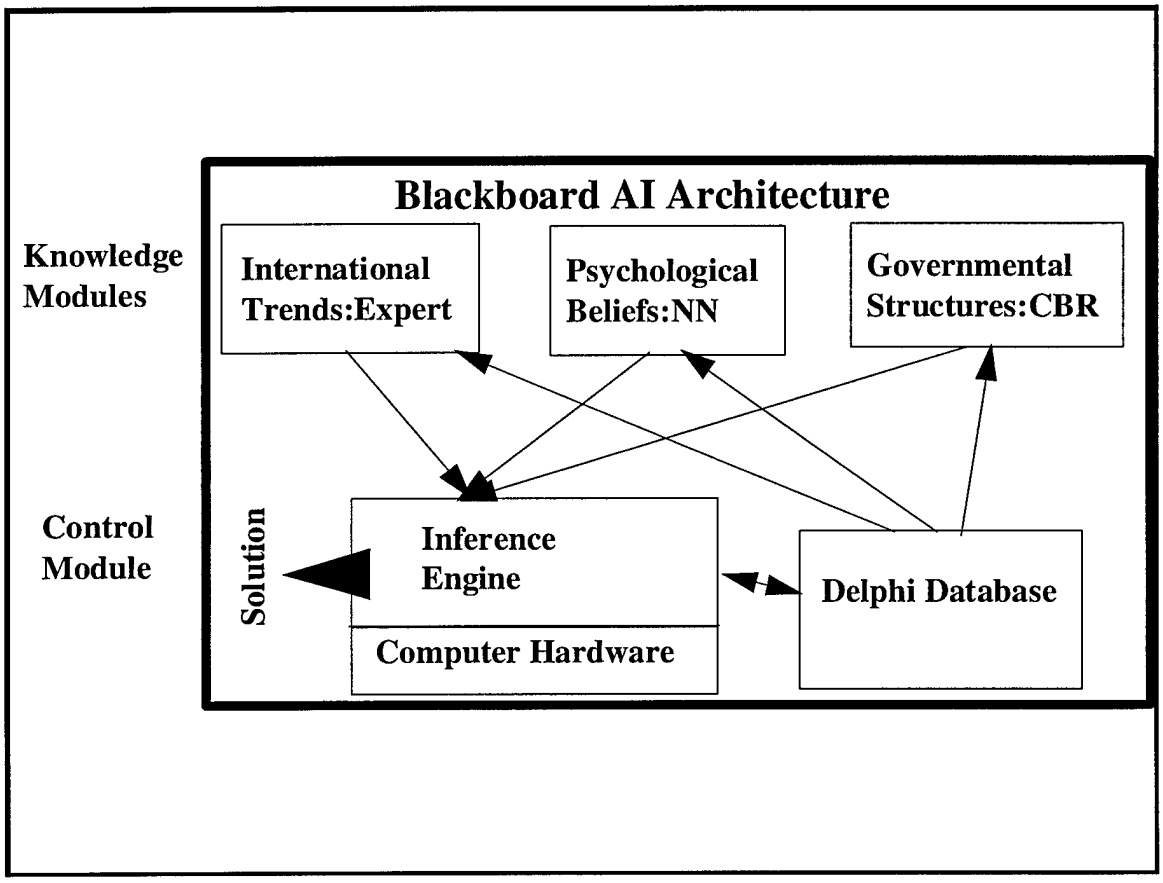


Figure 3-4. Artificial Intelligence Architecture

The blackboard is the part of computer memory that contains the control module and the knowledge modules. The knowledge modules are a collection of independent components that, when combined, provide the information necessary to solve the problem;. The modeler can choose the optimal AI technique for the problem being worked. Each knowledge module can function independently to determine an optimal solution for the problem that it is working.

The control module provides a vehicle for combining the outputs of the knowledge modules in order to arrive at a solution. It does this through the use of an "inference engine," an algorithm combining AI technologies. The control module considers all contributions from each knowledge module, selecting only those that are appropriate at the time. It weighs each contribution according to its value rating. The control module is linked to the Delphi database to monitor its operation, directing data to specific knowledge modules through the use of software agents.[8] By monitoring the database, the control module ensures that significant events get routed to the proper place in priority fashion. It devises workarounds and graceful degradation strategies if parts of it fail.

In figure 3-4, the control module combines an expert system, a CBR system, and a neural network system to make decisions. The presence of the first two ensures that the system has the knowledge necessary to make the right call. The use of the neural network adds the ability to learn from past events. A promising scheme for combining these different AI approaches is Fuzzy Approximation Theory, which weights the methods by variable amounts based on the traits of the adversary and the situation.[9]

The blackboard system also enables the proposed AI solution to be "what if'd." Before proposing a COA, the blackboard expert inputs the decision to a world database residing in memory and games the likely consequence. This simulation process is iterated until arriving at a COA that generates an optimal solution. The solution is then provided to the human decision maker. The "gaming" feature is essential in order to explicitly consider the interdependent nature of world affairs. In *New World Vistas,* experts assert that by 2020 the fuzzy methods required by the inference engine of the "control module" will mature and the ability to "game" proposed COAs will exist.[10]

Before an AI system can be reliably employed, much improvement is required. The techniques employed above have been used only at very basic levels. A university professor developed an expert system to explain US foreign policy decisions made in Asia. When his model was backcasted to the 1950s it predicted a very favorable 86 percent of the decisions that the U.S. ultimately made.[11] CBR applications are being used commercially to handle customer service calls, with a technician asking the customer questions that take him through a fault isolation tree developed from past product failures.[12] Many examples of neural networks are in operation today.[13] Finally, the Navy uses blackboard systems to manage complex electronic

networks.[14] While these AI applications are simple compared to the requirements for 2025, they document the great strides being made in this field.

The AI portion of the system can be countered. AI requires the input of data to make decisions. If entered data is inaccurate or corrupted, the AI decisions will be degraded. Verifying the data and decisions for reasonableness minimizes this problem. Since the AI program operates in the electronic environment, it is subject to physical attack—either on the computers or on the electricity sources required to operate them. Steps to enhance the physical security of each major facility, combined with the distributed nature of the system, helps defend against these types of attacks. Finally, since AI is essentially a software-driven system, it is subject to information warfare attacks. This avenue of attack is best countered by an active counterinformation warfare capability.

Computer Hardware Requirements

The significant capability of the system analysis system of 2025 depends on improvements in computing capability.[15] Current processors cannot run the AI programs this system requires.[16] However, massive parallel Central Processing Unit (CPUs), where a large number of processors are combined on individual silicon chips, are being exploited commercially today. Again, there remains room for much growth.[17] Technical experts maintain that the current exponential growth in computing performance based on silicon technology will continue through 2006, at which point material constraint will force alternate methods. Promising alternate technologies include quantum, molecular, and optical computing methods.[18]

Target Acquisition System

In 2025, an organic relationship exists between target acquisition and the Delphi database. It is the classic "chicken or egg" relationship: the Delphi database must know the LOV exists before telling target acquisition sensors to find it; but the existence of the LOV may be discovered only after the target acquisition sensors collect initial data hinting at the LOV's existence. By necessity, therefore, the target acquisition phase operates continuously, passing streams of data to the Delphi database for analysis, while at the same time pulling fused information from the database to help guide the acquisition process.

The target acquisition system must provide decision makers the capability to detect changes in the personal values of an adversary. Changes in a leader's emotions, thoughts, or frame of reference are of interest to the strategic attack system. Techniques that get into the "head" of an adversary to obtain valuable information require revolutionary advances. Finding plausible methods for accomplishing this task is the focus of the classified "Information Attack" white paper. The target acquisition portion of strategic attack in 2025 complements these techniques with a diverse arsenal of sensor platforms.

Data collected by target acquisition sensors can range from single bits of data, like an LOV's exact location, to an entire library of data, such as the LOV's normal activity levels. In the year 2025, sensor collection provides enough data for a virtual 3-D model of the LOV to include its composition, internal structure, baseline characteristics, and tendencies. Using a biological warfare (BW) storage facility as an example, and in the most optimistic case, sensors determine the building's exact dimensions and floor plan. They then highlight possible soft spots. Sensors distinguish between rooms containing biological agents, test equipment, sleeping quarters, and even the snack bar.

Target acquisition sensors also construct a baseline, or living archive, of data concerning routine activity and environmental conditions. Examples include the average number of people who enter and exit each day, the number of vehicles in the parking lot, and the level of noise generated by the facility. This baseline data, combined with 3-D modeling, provides benchmarks for detecting changes in data collection; for example, a sudden increase in vehicular traffic or human activity.[19] Changes in an LOV's baseline activity data can be flagged to determine its significance. The AI system, or a human imagery analyst, can determine if the LOV requires a closer look by target acquisition sensors.

Target Acquisition Platforms

Target acquisition platforms in 2025 can be airborne, space-based, or ground-based. Function, cost, and vulnerability determine where to mount a sensor. It makes little sense to build expensive space platforms for sensors that work effectively from the ground.[20] On the other hand, some sensors may work effectively only above a certain altitude or from space. In any case, having a variety of platform types decreases an adversary's opportunity to completely stop sensor data collection and its transmission to the Delphi database.

A combination of commercial and military satellites should provide continuous worldwide coverage in 2025. Spatial resolutions of 10 meters, improved to two or three meters through signal-to-noise ratio calculations, will be available instantly and continuously.[21] In addition, expect multispectral, hyperspectral, and synthetic aperture radar images to provide periodic submeter resolution throughout a 24-hour span.[22] However, to obtain higher resolution images of LOVs on a *continuous* basis, airborne platforms must be employed.

Airborne sensor platforms can be described as standoff systems or overhead systems. A standoff system loitering along a political border at 50,000 feet can stare 230 miles downrange at an LOV and provide continuous one meter resolution.[23] Unmanned aerial vehicles (UAVs) or simple high altitude balloons could carry these sensors. In addition, a low observable UAV that loiters directly over a specific area will carry sensors that provide continuous one centimeter resolution.[24] The final type of sensor platform provides acquisition information that is unavailable from space-based assets.

Ground-based platforms in 2025 rely heavily on micromechanics and nanotechnology to shrink sensors and platforms to microscopic sizes.[25] These platforms could be inserted via human agents, through water or food supplies, or through aerial seeding operations using UAVs. Microsensors thinner than human hairs could transmit data to the Delphi database via UAV or satellite relay.[26] A swarm of ground-based microsensors could ensure constant data transmission of local conditions and activity levels near and inside an LOV.[27]

Except for micromechanical platforms, the *hardware* for most sensor platforms exists today. However, it is the sensors and not the platforms that collect the data to acquire the LOV. Therefore, the key to effective target acquisition in 2025 will be the development of critical sensor technologies. These technologies allow continuous collection of daytime, nighttime, and weather data that feeds the Delphi database to generate new LOVs.

Critical Target Acquisition Sensor Technologies

Successful target acquisition depends on critical sensor capabilities that will require much more development before the year 2025. To simplify their descriptions, the sensors can be compared to the human

ability to see, hear, smell, and taste. And just like in humans, the sensor data collected can be fused by the Delphi database to provide accurate information concerning LOVs. Traditionally, the "seeing" technologies dominated the sensor field using spectral analysis of the visual and infrared (IR) bands, along with SAR returns.[28] In 2025, radically different sensors add critical data to confirm or dispute what we think we "see." Having sensors that provide complementary data (instead of duplicating data) ensures better accuracy and reliability. It also prevents an enemy from defeating the entire system by destroying, or defending against, one type of sensor.[29]

Visual Sensors. Multispectral Imaging MSI currently dominates the sensor field. As mentioned before, the use of the visual and IR bands, plus SAR can provide resolution from 10 meters to one centimeter, depending on the platform distance from the LOV and loiter capability.[30] New technologies, like hyperspectral imaging, laser-light detection and ranging, and magnetic resonance imaging, can provide other methods to paint an LOV.

Instead of concentrating on a single broad-spectrum band, hyperspectral imaging involves slicing the entire electromagnetic spectrum into hundreds or thousands of single-wavelength data bands for collection.[31] The bands that produce a signature can be fused together by the Delphi database to construct a target signature.[32] LOVs may be able to avoid detection in one spectrum but not from all spectrums.[33] Due to size and weight, hyperspectral sensors will likely require airborne or space-based platforms.

Laser-based light detection and ranging (LIDAR) sensors offer great hope for detecting atmospheric changes due to chemical and biological reactions. By actively probing the atmosphere, LIDAR sensors will detect and construct 3-D images of aerosol clouds common to factories and machines. One can develop a best guess as to what a factory or machine produces by comparing predetermined aerosol images of known substances.[34] These sensors could also be used to warn of possible chemical and biological warfare agents on a battlefield. Future LIDAR sensors will easily fit in a small suitcase, making them adaptable for satellite and UAV platforms.[35]

Magnetic resonance imaging (MRI) is a sensor technology that is useful in building 3-D images of LOVs in 2025. An MRI sensor offers the advantage of imaging the internal, as well as external, structure of the LOV. UAVs could blanket a building with specially designed dust particles that circulate throughout the

structure's ventilation system.[36] Then MRI equipment and sensors carried on space-based or airborne platforms could scan the structure, analyzing the circulation of the dust particles to construct an internal image of the LOV.

Sound Sensors. Sound sensors can measure vibrations in the atmosphere or through materials. The ability to listen to human conversations using microphones mounted on space platforms may be available in 2025, but it will be expensive. A cheaper method involves miniature microphones built through micromachining. These sensors, the size of pinheads, could be planted via UAV seeding operations, human agents, or even letters sent through the mail.[37] The ability to listen to an LOV and its surrounding environment will provide early warning of an adversary's intention, especially when fused with the cues detected by visual sensors.

A second use for acoustical microsensors involves measuring seismic vibrations and mechanical resonance. Acoustic resonance spectroscopy can reveal the contents of sealed containers by analyzing the container's mechanical resonance.[38] Using a horde of tiny microphones, an entire structure could be analyzed and the data from each sensor relayed to the Delphi database via an overhead collector. These sensors could also be used for seismic mapping of underground facilities (like command bunkers) that escape detection by visual sensors.[39]

Smelling Sensors. In 2025, olfactory sensors will be similar in size to microscopic hearing sensors. Unlike the LIDAR system that detects signatures of aerosol clouds, smelling sensors can detect the actual chemicals themselves. Organic thin film coatings on tiny platforms will contain prefabricated "molecule buckets" to trap suspected chemical molecules. If the chemical is present, the buckets fill up, changing the organic property of the platform.[40] When irradiated by ultraviolet or X-ray energy, these organic changes can be scanned and analyzed by overhead sensors.[41]

Another novel smelling technology available in 2025 involves tracking humans via genetically-linked body odors.[42] These odors, undetectable by the human nose, can be sensed by bundles of sensors that then transmit the data to the neural network portion of the Delphi database. Since each sensor reacts differently to chemical compounds, specific compounds can be identified.[43] If it is possible to get an "odor" sample of an enemy leader, then olfactory sensors could be used to detect and track the human LOV.

Tasting Sensors. Sensors that transmit data after tasting an LOV can provide discriminating clues for the Delphi database in 2025. Tasting sensors can be prefabricated to detect--and attach to--certain types of surfaces, similar to the way smelling sensors have prefabricated molecule buckets. A variety of tiny taste sensors could be dispersed over an LOV, and then irradiated and scanned to gather data.[44] Taste sensors designed to detect aluminum would stick to aluminum aircraft wings but fall off wooden decoys. Other sensors could taste buildings or vehicles for radioactive fallout, chemical residues, or biological agents.[45]

If sensors can be designed to attach to specific compounds in 2025, they can be designed to attach to specific people. Like prickly cockleburs, tiny sensors would cling to certain humans, effectively tagging them for continuous tracking via overhead platforms.[46] If a human LOV cannot be tagged specifically, certain items common to that person, like vehicles and clothing, could be tagged for tracking. Possessing the ability to detect and track a human LOV adds greater flexibility to the strategic attack process.

A constellation of sensors provide the tools for detecting and tracking LOVs in 2025. These sensors form the backbone of the target acquisition phase, offering overlapping and complementary capabilities. The data collected is delivered to the Delphi database, where LOVs can be determined and courses of action formulated. When a decision is made to commence strategic attack, the target engagement platforms receive whatever information has already been collected. That information will include the LOV's description, location, weaknesses, strengths, and the suggested method of attack to achieve the desired effect.

Target Engagement System

The third component of the strategic attack process, is target engagement. It provides the method for generating strategic effects in 2025. The targets identified for strategic attack vary widely based on the adversary and the situation, and require a diverse arsenal of capability. This arsenal must include means to affect hard and soft LOVs directly/or indirectly, using lethal or nonlethal power, and within an immediate to indefinite time frame. Futuristic engagement systems and techniques such as holographic projection, noise and gravity fields, biomedical operations, psychological operations, military deception, and information attack are all possible. These innovative indirect means are discussed in the classified C^2 and Information

Attack white papers. As a complement to those indirect techniques, this paper focuses on target engagements that use direct attacks with lethal and nonlethal power.

In 2025, the effectiveness of an attack is a critical factor. In the *New World Vistas* Summary Volume, modeling experts showed that "if the effectiveness of the attacker is increased from one to five, and the initial forces are equal in number, the attacker will lose approximately 10 percent of the force while destroying the enemy entirely."[47] Since the ***2025*** Alternate Future study depicts a smaller US military in most cases, we need to significantly increase our attack effectiveness through improvements in weapons and delivery platforms.[48]

Weapons

By 2025, conventional explosive weapons will be more accurate and their explosive effectiveness per unit mass will be higher by a factor of ten than those of today.[49] The miniaturized munitions technology demonstration's (MMTD) goal is to produce a 250-pound munition that is effective against a majority of hardened targets previously vulnerable to only 2,000-pound munitions. A differential GPS/INS system will be an integral component of the MMTD to provide precision guidance. These guidance and smart fusing techniques will produce a high probability of target kill.[50] Self-targeting missiles will compliment the MMTD. These missiles have microoptics, aerodynamic actuator arrays, active skins, and microelectromechanical system (MEMS) technologies. The many advantages of these missiles include standoff capability and relatively cheap production costs.[51] Conventional weapons, however, will not provide the full range of options required in 2025.

Although many of the weapons used today will still be employed in 2025, directed energy weapons (DEWs) have great potential for strategic attack missions. The three general classes of DEWs are laser, radio frequency (RF), and energetic particle beam. They present an excellent complement to conventional weapons due to their characteristics. First, some DEWs have a higher probability of hit compared to projectiles. This is because the spreading beam can irradiate the entire target, therefore requiring less pointing and tracking accuracy. Second, they offer near-instantaneous engagement capability in most weather conditions. Third, each has a large magazine compared with the typical aircraft store of conventional

projectiles and missiles.[52] Fourth, DEWs have the potential to be much cheaper to support than conventional explosives. The traditional bomb loading, fusing, and storage facility could be replaced by the "fuel" required to source the DEW. Last, and maybe most important, DEWs can be nonlethal in some applications.

Lasers will be the first to become operational on our strategic attack platforms. Significant progress has already been made in the airborne laser (ABL) program, underway since 1992. The program gives the U.S. military a credible boost-phase defense against theater ballistic missiles. This laser is slated to be flight-tested in 2002 and fielded in 2006. Each laser shot is estimated to cost only $1,000 in "laser fuel," which is a mixture of common chemicals.[53] Cost-effectiveness is further enhanced by a single mission being able to deliver multiple shots prior to mission completion. Recent success in using high density polyethylene (HDPE) plastic in the chemical oxygen iodine laser (COIL) can save on material cost by a factor of 100 and on machining cost by a factor of three—all without degrading laser performance. Because it is nine times lighter than the metals normally used in constructing lasers, HDPE is an ideal choice for an airborne COIL platform.[54] Through techniques like these, we can make lasers small and light enough to become modular weapons systems on our strike platforms. Limitations of lasers include being fair-weather weapons and requiring dwell times in the range of seconds; however, RF weapons can be used to compensate for these weaknesses.

The RF weapon showing the most promise is the high power microwave (HPM). It is not limited by weather and requires less than a second of dwell time on a target. The HPM's effect on electronic devices ranges from disruption to destruction, depending on the target's electromagnetic susceptibility and the HPM parameters. Energy from an HPM weapon can couple into system electronics through front door or back door paths at frequencies that may be either in-band or out-of-band. This means that electronics can be burned out even when the system is turned off.[55] In general, the susceptibility of electronics to an HPM increases as the scale size of the electronics decreases, making the most modern electronic systems potentially the most vulnerable.[56]

High power microwave weapons also provide great flexibility in their lethality by having "dial-a-frequency" options. In most cases, the HPM could be targeted against electronic systems and be tuned to a frequency that would pass harmlessly through humans. On the other hand, if the situation required, the HPM

could be used against enemy personnel. It could be set at a low power to cause sufficient pain to stop enemy personnel, or "turned up" to actually burn troops to death.[57]

Both laser and HPM weapons have the added benefit of providing our platforms organic self-protection capability. Just as the ABL can engage theater ballistic missiles, our strike platforms could use their organic DEW weapons to destroy attacking missiles. The laser would require a direct hit, while the HPM weapon could be less accurate and still have the same positive results. The HPM approach also has the potential of being a "force shield" for the strike platform if engaged by multiple threats simultaneously.[58] The major disadvantage of HPM is the danger of fratricide, since US systems rely so heavily on electronics. Safeguards and procedures must be integrated in the weapon system to prevent this hazard.

Energetic particle beams offer the most potent form of DEW, since their penetrating power is robust against the most stringent hardening measures.[59] As an analogy, using lasers and HPMs is like shooting BBs at a target while the particle beam is like firing baseballs. Unfortunately, the atmosphere significantly degrades the particle beam's propagation over long ranges and limits its usefulness on earth. Since similar atmospheric propagation problems do not exist in space, and MEMS developments will shrink the size of these weapons appreciably, it is likely that energetic particle beams can be used to conduct strategic attacks against enemy LOVs in space.

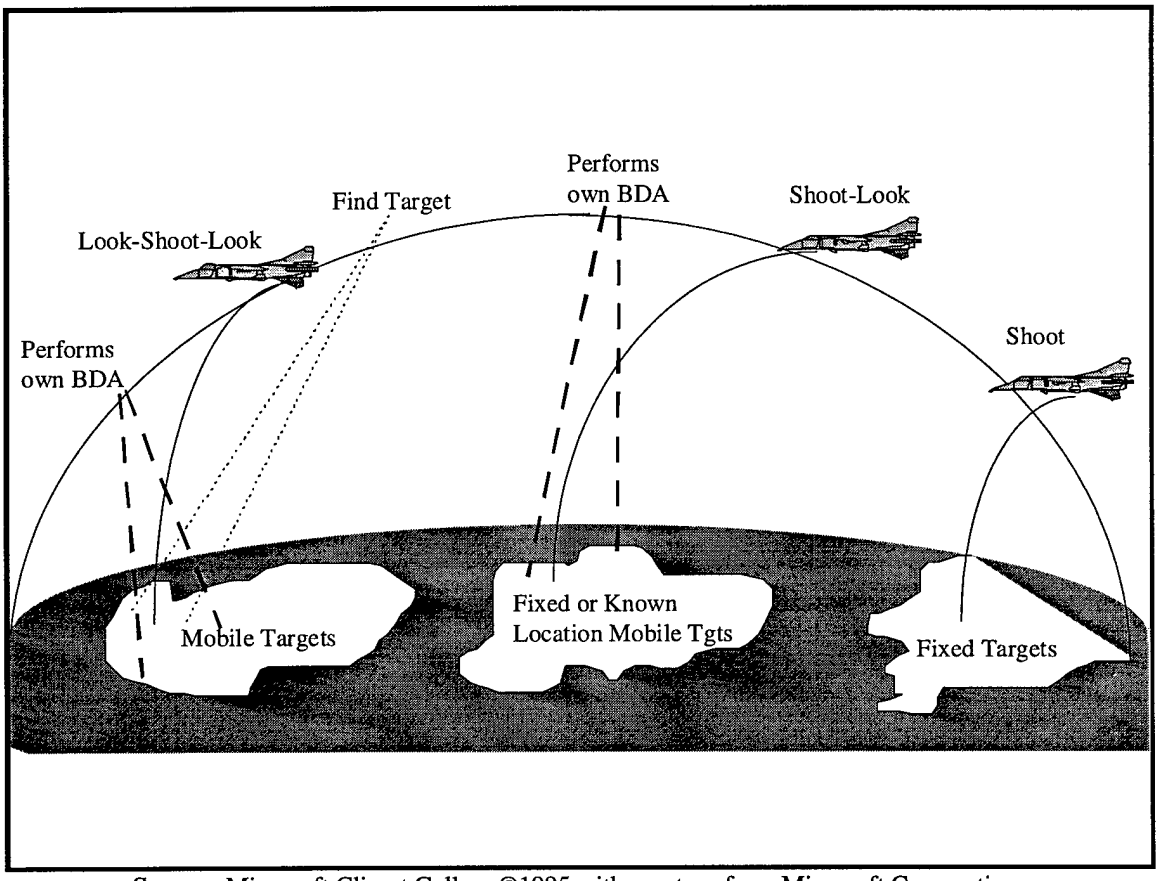
Strategic Platforms

Strategic attack platforms will involve UAVs, transatmospheric vehicles (TAVs), and space-based systems. UAVs will be prevalent in the future, and many of them will support the strategic attack mission. Their benefits and specifications are detailed in the 2025 UAV white paper. Because the UAV has a slow response time, newer platforms like the TAV and space-based systems are required. TAVs and space-based platforms can satisfy the portion of strategic attack in 2025 that requires immediate and massive firepower to accomplish great shock value.

The 2025 Spacelift and "Through the Looking Glass" white papers provide the specifications of a plausible force application TAV and space-based weapons. However, many of their characteristics are restated in this paper because they directly support the strategic attack mission. The TAV would be capable-- from an alert posture-- of arriving at a target anywhere in the world within one hour of notification. Its

weapons bay would be modular to allow several different types of weapons for increased flexibility. TAVs returning from a mission could be serviced and ready to fly again in less than a day, and could be surged to fly multiple missions per day if necessary.

The TAV platform capitalizes on several principles of war. It is offensive, bringing the fight to the enemy on our terms. The TAV provides surprise, striking enemy targets at any depth with little or no warning. Additionally, it delivers massed effects by employing precise firepower. Just as the F-117 carrying PGMs delivered on the principles of mass and economy of force during the Gulf War, the TAV will take this one step further. This platform accomplishes multiple attacks over a diverse target set during a single mission. Ultimately, with the appropriate weapons load, it can engage targets in separate major regional contingencies during a single mission. (fig. 3-5). In short, the TAV provides a timely threat to strategic targets anywhere on the globe.



Source: Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

Figure 3-5. Transatmospheric Vehicle

The vehicle must be designed to incorporate a modular weapons system. This concept increases cost effectiveness by allowing the TAV to be used for a variety of military missions, from force enhancement through force application. These weapon modules are maintained in readiness, stored until needed, and then quickly loaded on the vehicle. Finally, better sustainability can result from quick reloads and rapid turn-times, The TAV will provide quick reaction time across the globe; however, some cases will require more immediate strategic attack.

Utilizing a space-based platform is a powerful strategic attack option because it truly provides an "anytime. . .anywhere" engagement capability. Two generic deployment strategies exist. The first is an autonomous weapon deployed in space along with beam directing optics and control systems. This approach creates significant problems due to space logistics, resupply, targeting, and control. Additionally, it raises political issues related to the placement of offensive power in space. These technological difficulties and political issues make a second deployment option more attractive.[60]

Constructing a DEW on the ground and deploying targeting mirrors in space is the more feasible option. Having the source of energy on the ground means that laser energy will not be limited by satellite power or by available fuel. The large targeting mirrors, built with lightweight structures, could employ wave front compensation to correct for optical imperfections.[61] These spaced-based mirrors provide the capability to immediately apply lethal and nonlethal DEWs on a strategic LOV.

Feedback Systems

The last ingredient of the organic strategic attack process is feedback. Feedback provides the Delphi database with a near-instant awareness of an LOV's status. It answers the question as to the outcome of the strategic attack: Did the mission achieve success, failure, somewhere in between, or overkill? Knowing how much or how little an LOV was affected allows the system analysis network to generate subsequent courses of action.

Traditionally, feedback in the strategic attack process has been called battle damage assessment (BDA). In 2025, strategic attack may not involve "battle" with an enemy to inflict "damage" to its personnel and

equipment. Nonetheless, the "assessment" part of BDA remains a constant requirement for efficient and effective strategic attack.

The platform and sensor capabilities required for feedback in strategic attack are the same as those discussed in the target acquisition phase. This further illustrates the organic nature of the strategic attack process as a whole. The visual sensors placed on space and airborne platforms can provide continuous multispectral images of LOVs. However the importance of visual sensors may decrease in 2025 as the strategic attack process relies more on nonlethal methods of attack. In this case, non-traditional sensors that can hear, smell, or taste become essential by providing important bits of data that allow the Delphi system to piece together the effectiveness of an attack.

Notes

[1] ***2025*** Concept, no. 900374, "Living World-Wide Intelligence Data Basing," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[2] Joseph W. Wilkinson, *Accounting Information Systems: Essential Concepts and Applications,* 2nd ed. (New York: John Wiley & Sons, 1993), 219-221.

[3] USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century,* summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 87.

[4] Ibid.

[5] John W. Griesser, "Experts Among Us," *Business Horizons* 35, no. 3 (May-June 1992): 77-80.

[6] J.J. Daniels and E.L. Rissland., "A Case-Based Approach to Intelligent Information Retrieval," 1995. On-line Internet, 3 January 1996, available from http://cbr-www.cs.umass.edu/abstracts.html#Daniels:CBR-Approach-to-IR.

[7] Peter J. Denning, Neural Networks," *American Scientist* 86, no. 4, (July-August 1992): 426-429.

[8] ***2025*** Concept, no. 900446, "Automated Enemy Analysis Software," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[9] Bart Kosco, *Fuzzy Thinking, The New Science of Fuzzy Logic*, (New York: Hyperion, 1993), 156-223.

[10] *New World Vistas,* summary volume, C1-C15. The study suggests that the best approach for using software agents in this fashion is to have the agent generate specific data/task requests, rather than have it remotely travel the distributed database.

[11] Charles S. Taber, "POLI: An Expert System of U.S. Foreign Policy Belief Systems," *American Political Science Review* 86, no. 4 (December 1992): 888-904.

[12] Daniels and Rissland.

[13] Denning, 426-429.

[14] Randall J. Calistri-Yeh, "Applying Blackboard Techniques to Real-Time Signal Processing and Multimedia Network Management," *Proceedings of the 7th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems*, June 1994 (Austin, Tex.: IEA/AIE), 593-599.

[15] ***2025*** Concept, no. 900397, "Multi-Concurrent Operations CPU," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[16] ***2025*** Concept, no. 900791, "Quantum Mechanical Computer," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[17] George Gilder, *Microcosm*, (New York: Simon & Schuster, 1989), 319-330.

[18] *New World Vistas,* summary volume, 90.

[19] Oscar Firschein, "Defense Applications of Image Understanding," *IEEE Expert*, October 1995, 11-17..

[20] *New World Vistas,* summary volume, 22.

[21] Ibid., 21.

[22] Ibid.

[23] Ibid., 22

[24] Ibid.

[25] Gary Stix, "Micron Machinations," *Scientific American,* November 1992, 107.

[26] Naomasa Nakajima, "Micromachines," *The Futurist,* January 1994, 50.

[27] ***2025*** Concept, no. 900288, "Swarms of Micro-Machines," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[28] "Leveraging the Infosphere: Surveillance and Reconnaissance in 2020," *Airpower Journal 2,* vol. 9 no. 2 (Summer 1995): 14.

[29] Ibid., 12.

[30] *New World Vistas,* summary volume, 21.

[31] ***2025*** Concept, no. 900215, "Weather Data Collection/Display," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[32] "Leveraging the Infosphere: Surveillance and Reconnaissance in 2020," 15.

[33] USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century* (unpublished draft, the sensors volume, 15 December 1995), vi.

[34] William B. Scott, "LIDAR System to Detect Biological Warfare Agents," *Aviation Week & Space Technology,* vol. 143, no. 2 (13 November 1995): 44.

[35] Michael Black, "Technology's Brightest Stars," *R&D Magazine: The International Magazine of Research and Development (* October 1993), 58.

[36] "Leveraging the Infosphere: Surveillance and Reconnaissance in 2020," 12.

[37] David E. Newland, "Acoustic Micromachines," *Nature,* vol. 370, no. 6484 (7 July 1994): 21.

[38] "Three DOE Devices Will Assist in Weapons Dismantlement," *R&D Magazine: The International Magazine of Research and Development (* September 1995), 36.

[39] "Leveraging the Infosphere: Surveillance and Reconnaissance in 2020," 17.

[40] Barbara Smith, "Technology Takes the Pinch Out of 'Going Green'," *R&D Magazine: The International Magazine of Research and Development* (September 1995), 45.

[41] *New World Vistas,* (unpublished draft, the sensors volume), 164.

[42] Clive Cookson, "The Rise of the Robot Nose," *World Press Review,* vol. 42, no. 9 (September 1995): 36.

[43] Otis Port, "A Nasal Network to Sniff Out Friend or Foe," *Business Week: Industrial/Technology Edition,* no. 3454 (11 December 1995): 115.

[44] *New World Vistas,* (unpublished draft, the sensors volume), 164.

[45] "Leveraging the Infosphere: Surveillance and Reconnaissance in 2020," 18.

[46] ***2025*** Concept, no. 900469, "Hitchhiking Sensors," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

[47] *New World Vistas,* summary volume, 7. The importance of this quote is as a point of contrast for the expanded engagement capabilities that attack platforms will need in 2025.

[48] Maj John Geis, et al., "Alternate Futures," briefing (Air War College, Maxwell AFB, Ala.: 13 February 1995).

[49] *New World Vistas,* summary volume, 9.

[50] Lt Col Ted O. Mundelein, "Miniaturized Munition Technology Demonstration," (Unpublished paper, Eglin AFB, Fla.: January 1996).

[51] Terry Neighbor, "Wright Laboratory 2025 Technologies Air Power Day," 2025 Lecture (Air War College, Maxwell AFB, Ala.:), 13 November 1995.

[52] John T. Tatum, "A New Threat to Aircraft Survivability: Radio Frequency Directed Energy Weapons," *Aircraft Survivability*, Fall 1995, 11.

[53] Steve Watkins, "Service Closes in on an Airborne Laser," *Air Force Times*, 21 August 1995, 25.

[54] Phillips Laboratory Computational Services Division, "Plastic Fabrication of Chemical Oxygen Iodine Laser (COIL) Devices," Phillips Laboratory, on-line, Internet, 25 March 1996, available from http://www.plk.af.mil/SUCCESS/coil.html.

[55] Dr William L. Baker, "Air Force High-Powered Microwave Technology Program," *Aircraft Survivability*, Fall 1995, 9.

[56] Ibid., 9.

[57] Col William G. Heckathorn, "Advanced Weapons and Survivability Directorate Vision," 2025 Lecture, Air War College, Maxwell AFB, Ala.: 4 Dec 1995.

[58] Baker, 9.

[59] Dr Louis C. Marqet, "Aircraft Survivability and Directed Energy Weapons," *Aircraft Survivability*, Fall 1995, 7.

[60] *New World Vistas,* summary volume, 47–48.

[61] Ibid., 47.

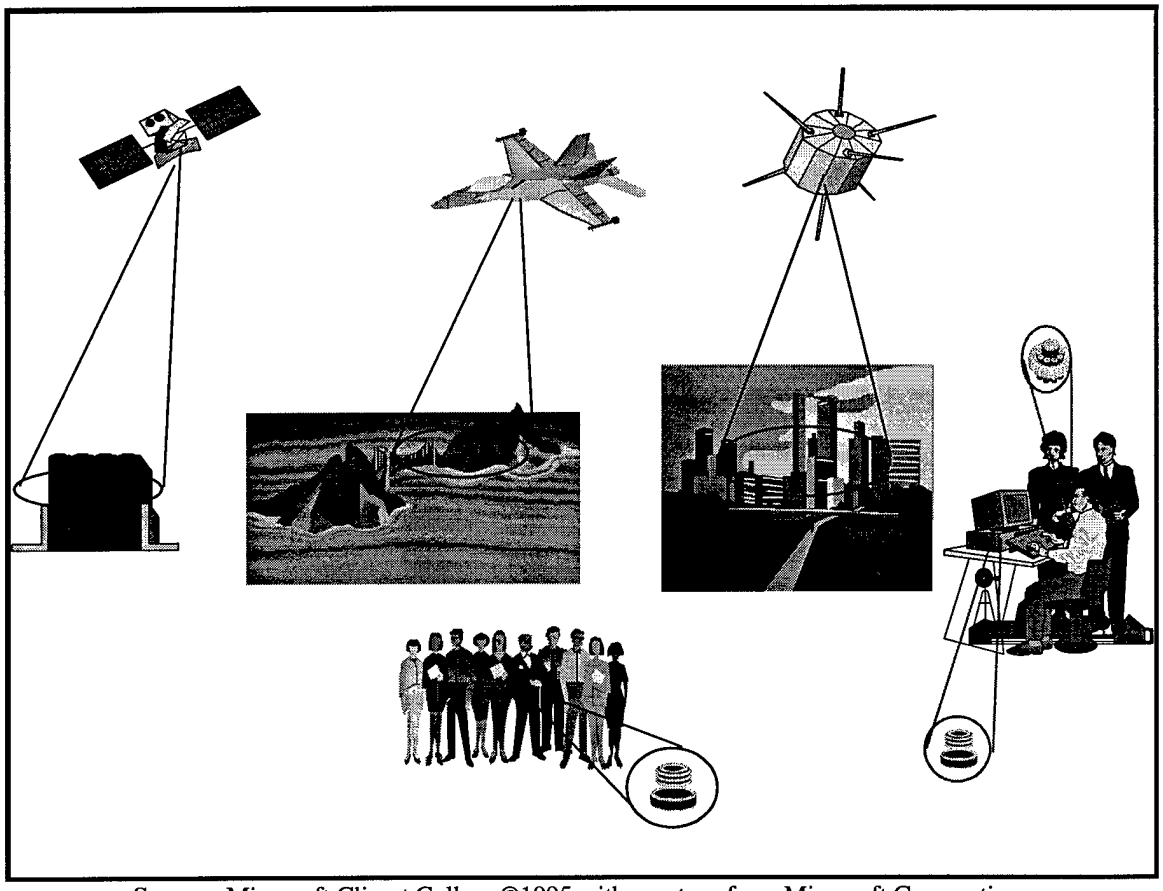
Chapter 4

Concept of Operations

The goal of strategic attack in 2025 is to conduct operations "to a point where the enemy no longer retains the ability or will to wage war or carry out aggressive activity."[1] Those operations run the gamut from traditional, highly destructive, force-on-force encounters to much less invasive, but very effective computer-based warfare. In 2025, advances in technology will improve the ability of the US to bring air and space power to bear on an adversary to achieve such war-winning effects. A description of the 2025 strategic attack system follows, based upon the technologies and organization outlined in the body of this paper. This system has four organically-linked components: a system analysis system, a target acquisition system, a target engagement system, and a feedback system.

Data from all over the world, in virtually every form, is monitored by the system analysis system. This collection of databases, called the Delphi system, is managed by advanced AI technology. As world developments occur, the AI portion of the system determines which databases contain useful facts. The data originates from various military, commercial, and institutional sources. The Delphi system analyzes this data and determines solutions to the strategic problem in terms of what LOV to target and how to affect it. It feeds that information to human decision makers and the target acquisition system.

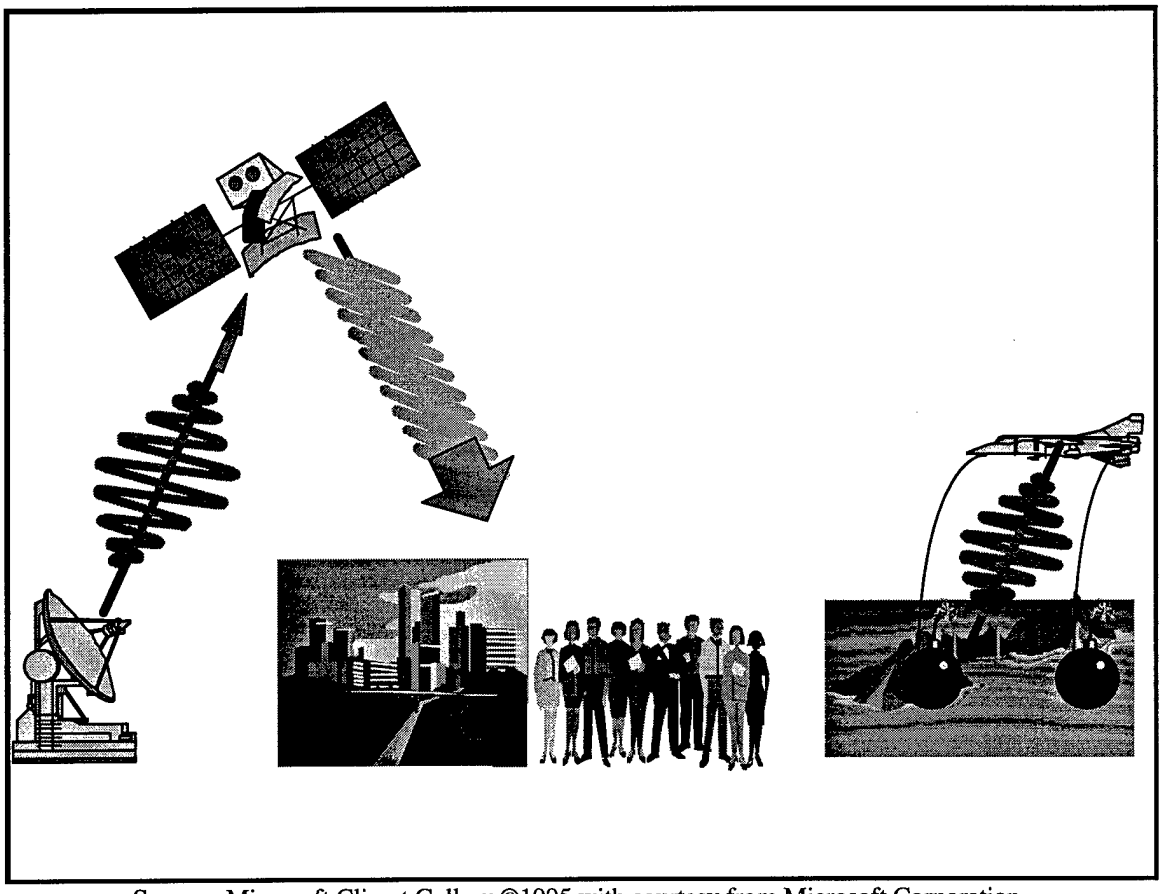
The target acquisition system in figure 4-1 uses sophisticated visual imaging and acoustical sensors to collect data from airborne platforms. It also employs ground-based microsensors to gather additional facts. It updates the Delphi database by providing LOV characteristics, such as location and composition, and makes this information available to the target engagement system.



Source: Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

Figure 4-1. Notional Target Acquisition System

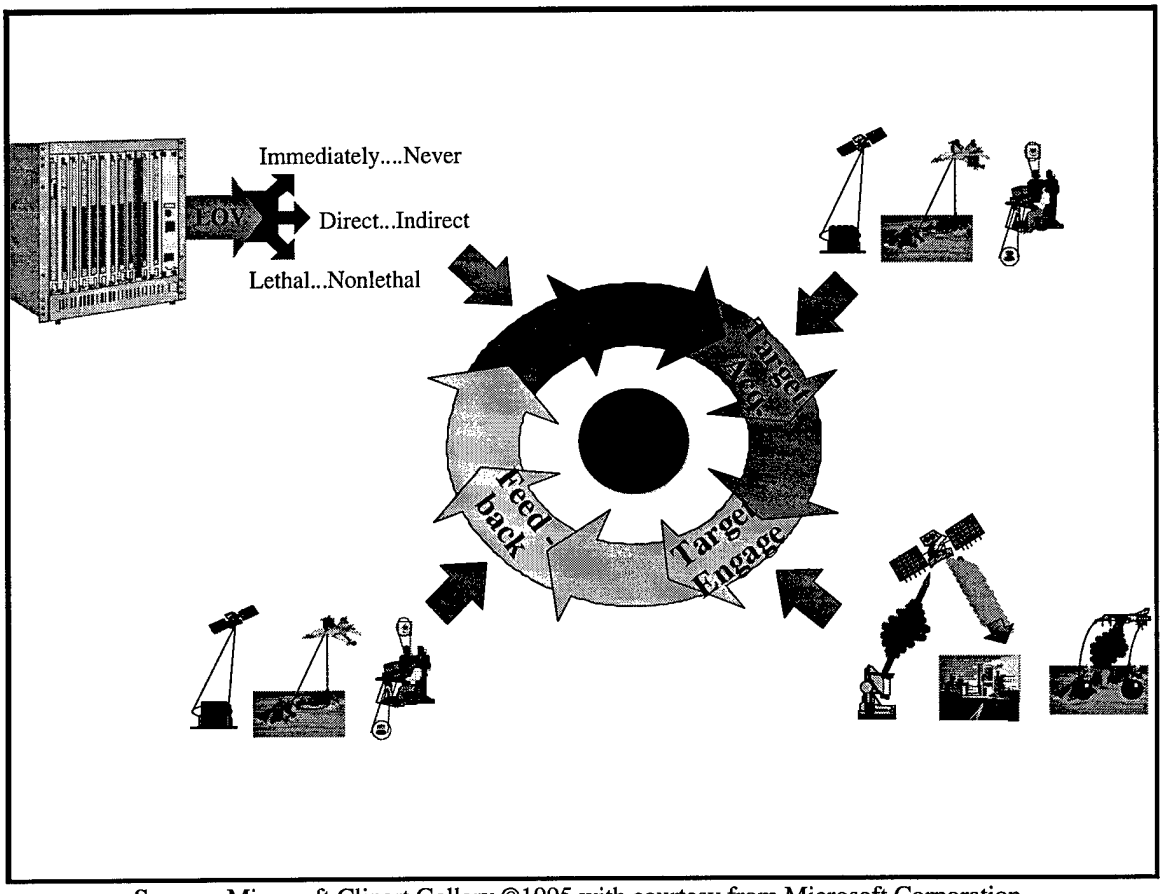
Once national authorities decide to implement the recommendations provided by the Delphi system, the target engagement system depicted in figure 4-2 is employed. The engagement system encompasses a broad range of tools to conduct psychological operations, perform computer-based attacks, deliver powerful conventional weapons from TAVs and UAVs, and utilize DEWs from space. This paper concentrated on attacking physical LOVs; however, as mentioned earlier, strategic effects can come from many approaches. This physical attack focus is intended to complement other **2025** white papers that detail innovative approaches for affecting less tangible LOVs.



Source: Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

Figure 4-2. Notional Target Engagement System

The targeting system queries the Delphi database for the information necessary for engagement. The database delivers this product after updating relevant information by communicating with the sensor arrays feeding the acquisition system. Based on the desired effect the targeting system selects the proper platform and weapon for the LOV. During and after the attack, the acquisition system monitors the target and reports its status to the Delphi system. Delphi uses its AI component to determine the degree of target engagement effectiveness. Delphi then reports that information to national leaders, along with the next recommended course of action. The outcome is a series of precise attacks with effects across the depth and breadth of an adversary. Figure 4-3 depicts the total strategic attack system.



Source: Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

Figure 4-3. Strategic Attack in 2025

Notes

[1] Department of the Air Force, *Air Force Doctrine Document 1, Air Force Basic Doctrine* (draft) (Langley AFB, Va.: USAF Doctrine Center, 15 August 1995), 13.

Chapter 5

Investigative Recommendations

Examination of the required capabilities for a strategic attack system in 2025 revealed several high pay-off technologies. Chief among the critical requirements are computing ability, artificial intelligence, nanotechnology, directed energy weapons, and transatmospheric vehicles.

At the foundation of the strategic attack system lies the continued improvement in computational and data storage ability. These two required capabilities are found throughout the organically-connected subsystems of strategic attack. While critical, these technologies should not be the focus of military research and development efforts. The rapid, global growth of information-based societies recognize this as a lucrative area for private investment. Scarce DOD dollars should be spent elsewhere.

Sophisticated AI advances are necessary. AI applications and a branch of AI, intelligent software agents, are critical keys to building a Delphi system that provides decision makers with the information to make optimal decisions in 2025. The military will not be alone in its quest to advance AI; many segments of the commercial sector also plan to use it. Improved profit opportunities motivate industries to invest in this area. The task of military leaders and long-range planners is to determine what unique military applications exist in the field, and then selectively fund them.

Selective funding is also required to exploit the budding science of nanotechnology. This technology forms the baseline for some sensors and weapons that the strategic attack system requires. Microsensors used for tagging potential targets, or scattered to monitor specific areas, rely heavily upon nanotechnology. Further, this capability creates smaller weapons for use on UAVs or TAVs.

Another potentially high return area of technology concerns directed energy weapons. DEWs offer a flexible, timely, affordable means to affect an adversary's LOV. They can be "tuned" for a wide range of

effects, from low-order intervention to high-order destruction. Additionally, the low cost of DEWs makes them cost effective. Finally, the speed, ubiquity, and aura of power associated with DEWs provide significant flexibility in execution and have a profound deterrent value.

The TAV is yet another important enabling technology. The TAV retains the flexibility and on-the-fly innovation of manned vehicles. Further, the TAV's inherent speed allows for rapid engagement time. Finally, CONUS-based TAVs shrink the logistical tail, reduce security exposure, and create virtual global presence. The DOD should develop the TAV concurrently with the private spacelift industry.

Chapter 6

Conclusions

Strategic attack has always held a position of importance in the conduct of warfare. Done correctly, strategic attack shortens the fighting and reduces the costs. All warriors dream of conducting it with decisive effect, yet few have been successful. The difficulty usually centers on determining, locating, or engaging the correct LOV. This white paper identifies the most promising technologies and combines them to form an organic system for conducting strategic attack in 2025. Embracing these concepts provides a "hit'em where it hurts" capability to successfully prosecute strategic attack.

Bibliography

Baker, William L. "Air Force High-Powered Microwave Program." *Aircraft Survivability*, Fall 1995, 9.

Black, Michael. "Technology's Brightest Stars." *R&D Magazine: The International Magazine of Research and Development*, October 1993, 58.

Calistri-Yeh, Randall J. "Applying Blackboard Techniques to Real-Time Signal Processing and Multimedia Network Management." *Proceedings of the 7th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems*, June 1994, 593-599.

Clausewitz, Carl von. *On War*. ed. and trans. Michael Howard and Peter Paret. Princeton, N.J.: Princeton University Press, 1976.

Cookson, Clive. "The Rise of the Robot Nose." *World Press Review*, vol. 42 no. 9 (September 1995): 36.

Daniels, J.J. and Rissland, E.L. "A Case-Based Approach to Intelligent Information Retrieval." on-line, Internet, 3 January 1996, available from http://cbr-www.cs.umass.edu/abstracts.html#Daniels:CBR-Approach-to-IR.

Denning, Peter J. "Neural Networks." *American Scientist*, vol. 86 no. 4 (July-August 1992): 426-429.

Department of the Air Force. *Air Force Doctrine Document 1, Air Force Basic Doctrine* (draft). Langley AFB, Va.: USAF Doctrine Center, 15 August 1995.

Firschein, Oscar. "Defense Applications of Image Understanding." *IEEE Expert*, October 1995, 11-17.

Gilder, George. *Microcosm.* New York: Simon and Schuster, 1989.

Griesser, John W. "Experts Among US." *Business Horizons,* vol. 35 no. 3 (May-June 1992): 77-80.

Grinter, Lawrence E. and Schneider, Barry R. *Battlefield of the Future*. Maxwell AFB, Ala.: Air University Press, 1995.

Kosco, Bart. *Fuzzy Thinking, The New Science of Fuzzy Logic.* New York: Hyperion, 1993.

"Leveraging the Infosphere: Surveillance and Reconnaissance in 2020." Airpower Journal 2, vol. 9 no. 2 (Summer 1995): 10-25.

Marqet, Louis C. "Aircraft Survivability and Directed Energy Weapons." *Aircraft Survivability,* Fall 1995, 7.

McKitrick, Jeffrey, James Blackwell, Fred Littlepage, George Krans, Richard Blanchfield, and Dale Hill. "The Revolution in Military Affairs" in *Battlefield of the Future* edited by Barry R. Schneider and Lawrence E. Grinter. Maxwell AFB, Ala.: Air University Press, 1995.

Meilinger, Colonel Phillip. *10 Propositions Regarding Air Power.* Air Force History and Meums Program, 1995.

Mundellein, Ted O. *Miniaturized Munition Technology Demonstration.* Eglin AFB, Fla.: January 1996.

Nakajima, Naomasa. "Micromachines." *The Futurist*, January 1994, 50.

Newland, David E. "Acoustic Micromachines." *Nature,* vol. 370 no. 6484 (7 July 1994): 21-28.

Port, Otis "A Nasal Network to Sniff Out Friend or Foe." *Business Week: Industrial/Technology Edition*, vol. 3454 (11 December 1995): 115.

Scott, William B. "LIDAR System to Detect Biological Warfare Agents." *Aviation Week & Space Technology*, vol. 143, no. 2 (13 November 1995): 44.

Smith, Barbara. "Technology Takes the Pinch Out of 'Going Green'." *R&D Magazine: The International Magazine of Research and Development*, September 1995, 45.

Stix, Gary. "Micron Machinations." *Scientific American*, November 1992.

Szafranski, Colonel Richard. "Parallel War and Hyperwar: Is Every Want a Weakness," in *Battlefield of the Future* edited by Barry R. Schneider and Lawrence E. Grinter. Maxwell AFB, Ala.: Air University Press, 1995.

Tabor, Charles S. "POLI: An Expert System of US Foreign Policy Belief Systems." *American Political Science Review*, vol. 86, no. 4, (December 1992): 888-904.

Tatum, John T. "A New Threat to Aircraft Survivability: Radio Frequency Directed Energy Weapons." *Aircraft Survivability,* Fall 1995.

Toffler, Alvin and Heidi. *War and Anti-War.* New York: Little, Brown and Co., 1993.

2025 Concepts Database. Maxwell AFB, Ala.: Air War College/***2025,*** 1996.

"Three DOE Devices Will Assist in Weapons Dismantlement." *R&D Magazine: The International Magazine of Research and Development*, September 1995, 36.

USAF Scientific Advisory Board. *New World Vistas: Air and Space Power for the 21st Century,* Summary Volume. Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995.

———. *New World Vistas: Air and Space Power for the 21st Century,* Sensors Volume. Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995.

Watkins, Steve. "Service Closes in on an Airborne Laser." *Air Force Times,* 21 August 1995, 7.

Wilkinson, Joseph W. *Accounting Information Systems: Essential Concepts and Applications.* 2nd ed. New York: John Wiley & Sons, 1993.