AD-A285 478

DOCUMENTED BRIEFING

RAND

Future Technology-Driven Revolutions in Military Operations

Results of a Workshop

Richard O. Hundley, Eugene C. Gritton

DTIC
ELECTE
OCT 1 3 1994
S G D

National Defense Research Institute

Approved for public release;

DTIC QUALITY INSPECTED 5

94-32375

The research described in this report was sponsored by the Advanced Research Projects Agency under RAND's National Defense Research Institute, a federally funded research and development center supported by the Office of the Secretary of Defense, the Joint Staff, and the defense agencies, Contract MDA903-90-C-0004.

RAND
Copyright © 1994

The RAND documented briefing series is a mechanism for timely, easy-to-read reporting of research that has been briefed to the client and possibly to other audiences. Although documented briefings have been formally reviewed, they are not expected to be comprehensive or definitive. In many cases, they represent interim work.

RAND is a nonprofit institution that helps improve public policy through research and analysis. RAND's publications do not necessarily reflect the opinions or policies of its research sponsors.

Published 1994 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Internet: order@rand.org.

DOCUMENTED BRIEFING

RAND

Future Technology-Driven Revolutions in Military Operations

Results of a Workshop

Richard O. Hundley, Eugene C. Gritton

Prepared for the
Advanced Research Projects Agency

Accesion For
NTIS CRA&I
DTIC TAB
Unannounced
Justification
By
Distribution /
Availability Codes
Dist | Avail and / or Special
A-1

National Defense Research Institute

Approved for public release; distribution unlimited

PREFACE

From October to December 1992, RAND conducted a workshop for the Advanced Research Projects Agency (ARPA) on "Future Technology-Driven Revolutions in Military Operations." The purpose of this workshop was to identify technologies beyond the current ARPA research agenda that could bring about revolutions in military operations over the next 20 years and to outline the research efforts required to make a reality of new military systems based on these technologies.

This documented briefing summarizes the results of that workshop. It should be of interest to those involved in setting the course of future Department of Defense research and development activities.

This research was sponsored by the director of ARPA, and was conducted within the Acquisition and Technology Policy Center of RAND's National Defense Research Institute (NDRI). NDRI is a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, and the defense agencies.

CONTENTS

Preface iii

Summary vii

Acknowledgments xi

Section

1. Introduction 1
2. Very Small Systems 14
3. Biomolecular Electronics 42
4. New Technologies for Military Logistics 56
5. Cyberspace Security & Safety 64
6. Performance Enhancers for the Individual Soldier 76

Appendix

A. Participants in Workshop Sessions 89
B. Power & Energy Requirements for Mobile Microrobots: Order of Magnitude Estimates 97

Bibliography 103

SUMMARY

As Desert Storm has clearly shown, recent advances in technology have brought about dramatic changes in military operations, including the use of low-observable aircraft to negate air defenses, smart weapons for precision conventional-strike operations, and the employment of both ballistic missiles and antiballistic missiles in conventional warfare. Such technology breakthroughs will continue to occur in the future, just as they have in the past, and they will continue to bestow a military advantage on the first nation to develop and use them. Accordingly, it is important to the continued vitality and robustness of the U.S. defense posture for the Department of Defense (DoD) research and development (R&D) community, and in particular the Advanced Research Projects Agency (ARPA), to be on the leading edge of breakthrough technologies that could revolutionize future military operations. This may require additional research initiatives, as new technologies come to the fore. During October to December 1992, RAND conducted a workshop for ARPA on "Future Technology-Driven Revolutions in Military Operations," to identify candidate technologies for such research initiatives. This documented briefing summarizes the results of that workshop.

The workshop was conducted on a part-time basis over a several-month period, with an initial technology homework phase, two three-day working sessions in October and December 1992, a period of intermediate analysis between these sessions, and a postworkshop period to elaborate on the themes developed during the workshop sessions.

The workshop participants came from both the technology and military applications communities, and from both inside and outside of RAND. The RAND participants included researchers expert in military systems and operations, technology experts, and a number of the Air Force, Army, and Navy officers stationed at RAND as research fellows. These in-house participants were augmented by a number of consultants in relevant technology areas from both the academic and industrial research communities, and by a number of other consultants with expertise in post–cold war political and military environments and military operations. In total, 93 people participated in the workshop. (Appendix A lists the workshop participants.)

Seven technology areas, selected in consultation with ARPA, were considered during the first workshop session:

- Biotechnology and bioengineering
- Micro and nano technologies
- Future information technologies (including virtual reality)
- Autonomous systems (both large and small)
- Exotic materials
- Advanced energy and power technologies
- Advanced vehicle and propulsion technologies.

The intent of this technology menu was to span the likely future "revolutionary" possibilities—beyond the current ARPA research agenda.

Technology tutorials were prepared in each of the seven areas, with the assistance of the outside technology consultants, and presented to all of the workshop participants—military applications experts as well as technologists—at the beginning of the October 1992 workshop session, to stimulate their creative imaginations.

The workshop participants then split into a number of "concept groups"—mixtures of technologists and military applications experts, organized along military operations lines, across the political-military spectrum of expected future conflicts. Each of these concept groups was asked to create new application metaphors arising from the seven technology areas considered in the workshop.

This process led to the creation of a number of new application metaphors during the October 1992 workshop session. Five of these were selected for more in-depth consideration:

- The "Fly on the Wall"
  - Miniature fly-sized vehicles carrying a variety of sensors, for unobtrusive surveillance in a variety of military situations.
- Turning the "Fly" into a "Wasp"
  - Micro systems that disable enemy systems; a "fly with a stinger."

- The "Jedi Knight"
  - Multiple performance enhancements for the individual soldier.
- The "Smart Package" and the "Smart Logistic Highway"
  - New ways of doing military logistics.
- "Electronic Counterfeiting" and "Embedded Agents"
  - Counterfeiting of electronic information of all kinds.
  - Hardware and software "agents" embedded in a variety of information systems.

During the second session, working groups attempted to flesh out each of these five metaphors, sketching out system concepts and their possible impacts, and identifying the system performance and technology thresholds required for truly revolutionary impacts on military operations.

Since several of these metaphors involved very small—indeed, tiny—systems, another working group looked into the technical possibilities for power supplies for such systems. Still another group considered military applications of biotechnology, a subject that had raised much interest, but little closure, during the first session.

By means of this process, we identified four promising program areas as candidates for new ARPA research initiatives:

- Very Small Systems
  - The use of micro and nano technologies to develop miniature (e.g., fly-size) flying and/or crawling systems capable of a wide variety of battlefield sensor missions.
- Biomolecular Electronics
  - The use of techniques from molecular biology and biotechnology to develop new molecular electronic materials, components, and computational architectures.
- New Technologies for Military Logistics
  - The use of modern microelectronic and information technologies as the basis for a new advanced-technology military logistic system.

- Cyberspace Security and Safety
  - The development of techniques and strategies to protect U.S. interests in and relating to "cyberspace"—the global world of internetted computers and communication systems in which more and more U.S. activities (military and civilian, governmental and nongovernmental, economic and social) are being carried out.

The first three of these represent technological opportunities for ARPA. The fourth is an emerging national problem area, in which ARPA could play an important role.

We also identified a fifth area as a candidate for enhanced ARPA research efforts:

- Performance Enhancers for the Individual Soldier
  - The use of a variety of technologies to enhance the survivability, mobility, and mission performance of individual soldiers.

This documented briefing provides details on all five of these candidate program areas.

ACKNOWLEDGMENTS

The workshop on "Future Technology-Driven Revolutions in Military Operations" was truly a group effort. Its success resulted from the collaborative efforts of all of the participants, who are listed in Appendix A. They all deserve a major vote of thanks.

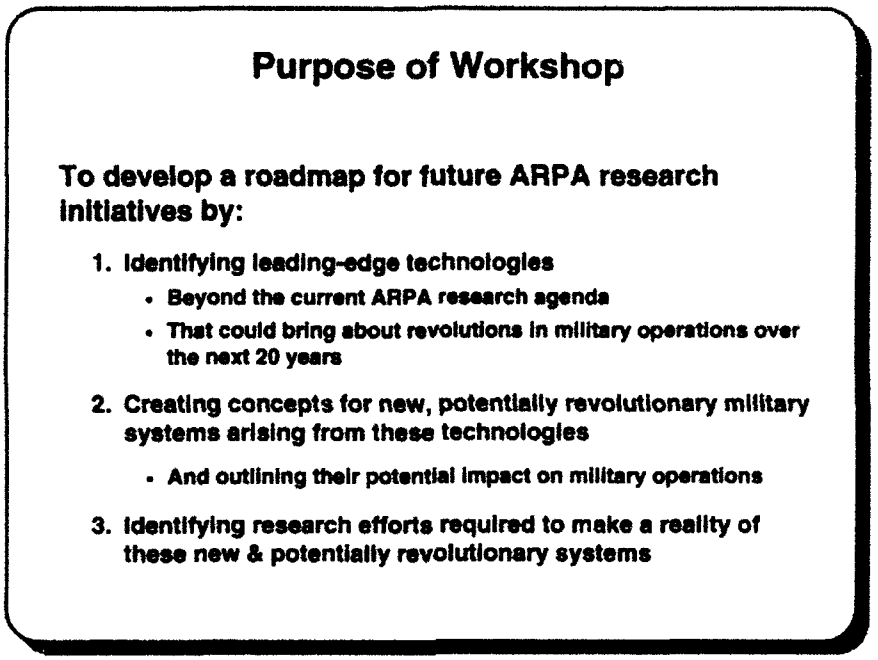
Special thanks go to the individuals who prepared technology tutorials: Robert Anderson, Bruno Augenstein, Keith Brendley, John Matsumura, Dan Raymer, Calvin Shipbaugh, and Randall Steeb; to the leaders of the concept groups at the October 21–23, 1992 session: Carl Builder, Fred Frostic, David Kassing, Richard Mesic, and Robert Moore; and to the leaders of the working groups at the December 14–16, 1992, session: Bruno Augenstein, James Bonomo, Keith Brendley, Carl Builder, Fred Frostic, Tony Hearn, John Hiland, Iris Kameny, David Kassing, Noel MacDonald, Robert Moore, Calvin Shipbaugh, Randall Steeb, and Robert Zimmerman. We would like to thank Bruno Augenstein, who prepared Appendix B, and Randall Steeb, who assisted with a portion of the main text.

We would also like to thank Colonel Randall Gressang, ARPA, who provided valuable guidance throughout the workshop process, and Dr. Gary Denman, the director of ARPA, without whose support the workshop would not have been possible.

1. Introduction

As Desert Storm has clearly shown, recent advances in technology have brought about dramatic changes in military operations: the use of low-observable aircraft to negate air defenses, smart weapons for precision conventional-strike operations, the employment of both ballistic missiles and antiballistic missiles (ABMs) in conventional warfare, and so forth. These dramatic technology-driven changes in military operations, recently termed the "military technical revolution," are not unique in the history of warfare, but merely the latest in a chain of "breakthrough technologies" extending back over time and including examples such as the ironclad ship in the 1860s, the machine gun in the 1890s–1910s, the manned aircraft and the tank in the 1920s–1930s, the aircraft carrier and radar in the 1930s–1940s, and nuclear weapons in the 1940s–1950s.

Such technology breakthroughs will continue in the future just as they have in the past, and they will continue to bestow a military advantage on the first nation to develop and use them. Accordingly, it is important to the continued vitality and robustness of the U.S. defense posture for the Department of Defense (DoD) research and development (R&D) community, and in particular the Advanced Research Projects Agency (ARPA), to be on the leading edge of breakthrough technologies that could revolutionize future military operations. This may require additional research initiatives, as new technologies come to the fore. During October–December 1992, RAND conducted a workshop for ARPA on "Future Technology-Driven Revolutions in Military Operations," to identify candidate technologies for such research initiatives. This documented briefing summarizes the results of that workshop.



The overall purpose of this workshop was to develop a roadmap for future ARPA research initiatives. To this end, the workshop pursued three specific objectives:

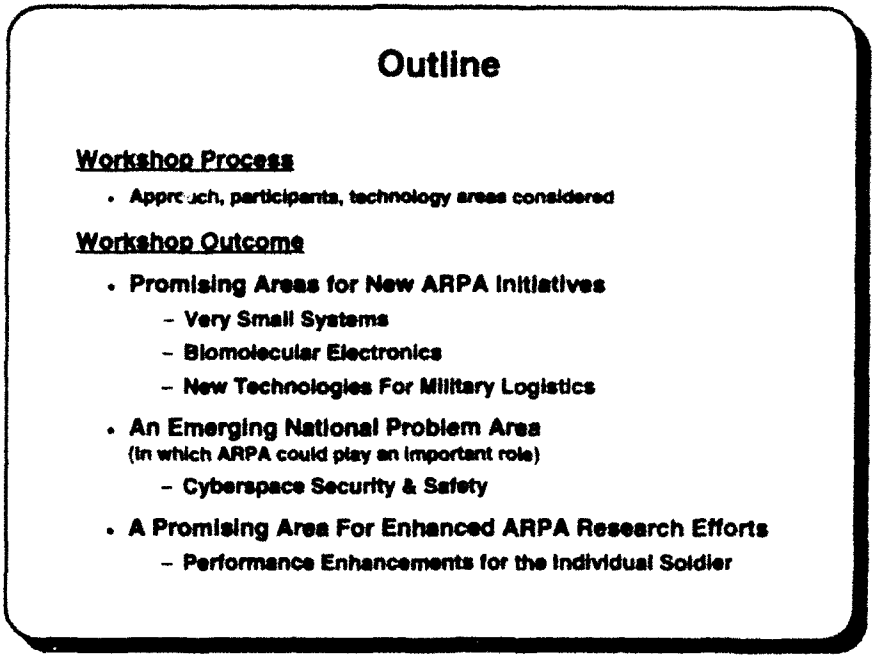
1. To identify an interesting set of leading-edge technologies, beyond the current ARPA research agenda, that could bring about revolutions in military operations over the next 20 years.[1]

2. To conceptualize potentially revolutionary military systems arising from these technologies, and identify/illustrate the nature of their possible impact on military operations.

3. To identify the research efforts required to make a reality of these new and potentially revolutionary systems.

---

[1]We did not try to be all-inclusive in the technologies selected, but rather to identify a small number of technologies that appear to have the potential for revolutionary effects.



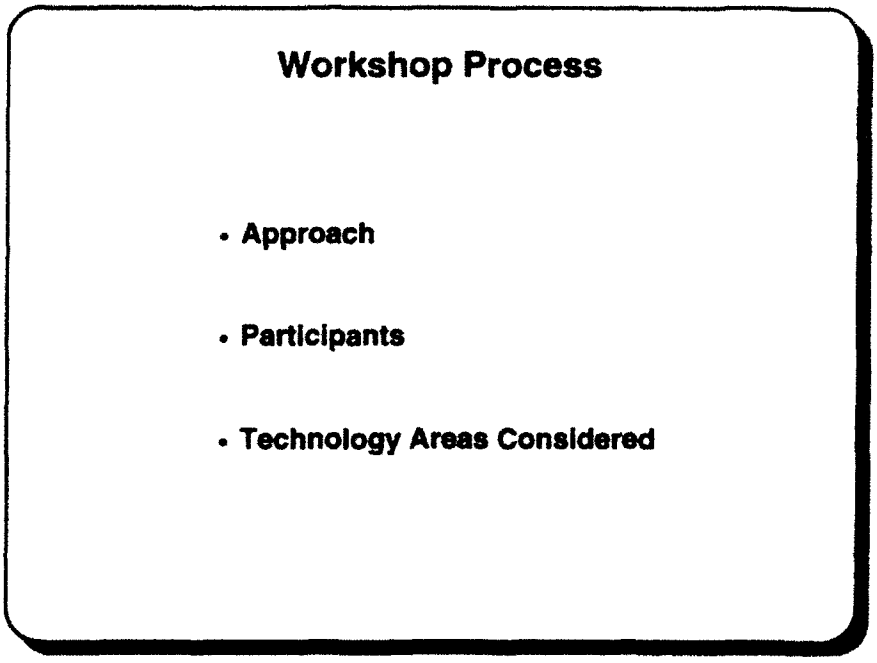
This documented briefing begins with a brief discussion of the workshop process: the approach used, the technology areas considered, and the participants who were involved.

Following that, the bulk of the report focuses on the workshop outcome—the four research areas identified during the course of the workshop as candidates for new ARPA initiatives:

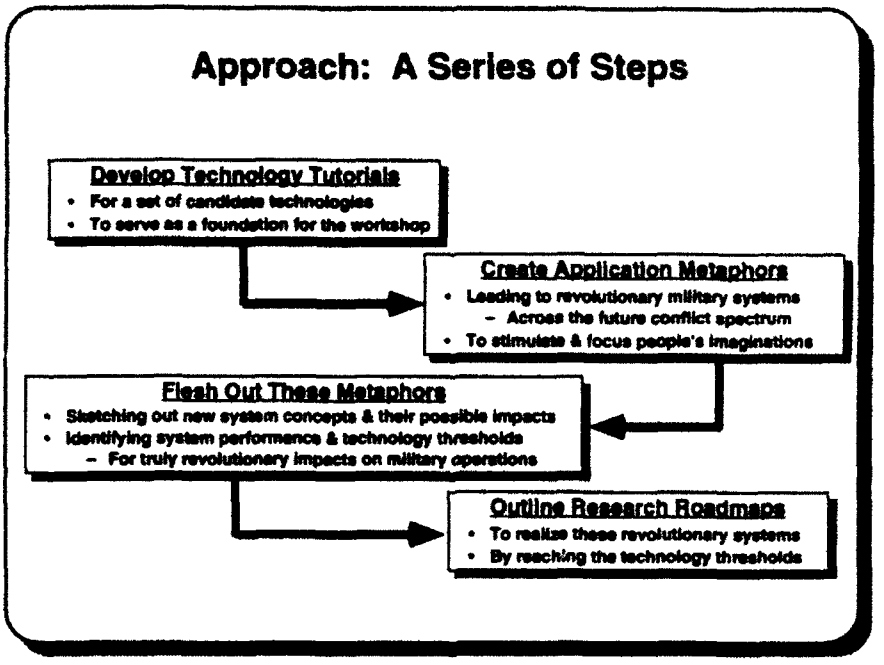
- Very small systems
- Biomolecular electronics
- New technologies for military logistics
- Cyberspace security and safety

and a fifth area identified as a candidate for enhanced ARPA research efforts:

- Performance enhancers for the individual soldier.

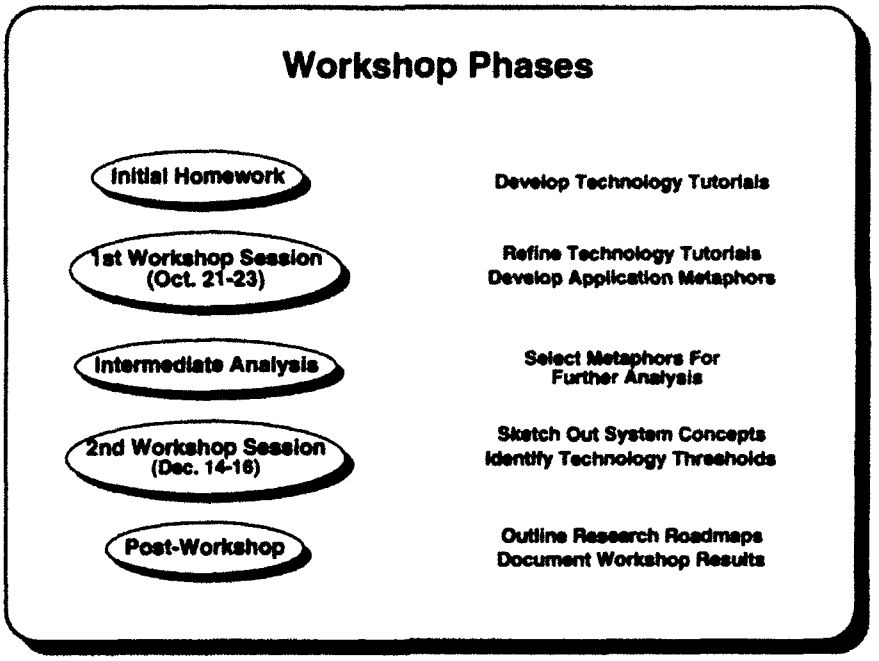


We begin with a discussion of the workshop process.



The intellectual approach used during the workshop involved four sequential steps:

- Development of a number of "technology tutorials"—i.e., overviews of current research activities, future research directions, and possible future technology capabilities— in a number of technology areas, to serve as the intellectual foundation for subsequent workshop activities.
- Creation of new "application metaphors" arising from these technologies that potentially could lead to revolutionary military systems.
- Fleshing out of the most promising of these metaphors, to sketch out system concepts and their possible impacts, and to identify the system performance and technology threshold required for truly revolutionary impacts on military operations.
- Outline of the research steps necessary to reach these technology thresholds and realize these revolutionary systems.



The workshop had a series of phases, extended over a several-month period:[2]

- An initial homework phase, to develop the technology tutorials.
- The first workshop session, on October 21–23, 1992, which refined the technology tutorials and developed a series of application metaphors.
- A period of intermediate analysis, during which a subset of the most promising of these metaphors was selected for further analysis.
- The second workshop session, on December 14–16, 1992, which sketched out system concepts for the selected application metaphors and their likely impact on military operations, and identified the key technology developments required to make these systems a reality.
- A postworkshop period, during which a final set of the most promising/challenging research areas coming out of the workshop process were selected as candidates for new ARPA initiatives.

---

[2]In recent years, RAND has conducted several of these extended, part-time workshops. We have found them to be much more effective, for the same overall expenditure of effort, than one-shot, "crash" sessions.

Workshop Participants

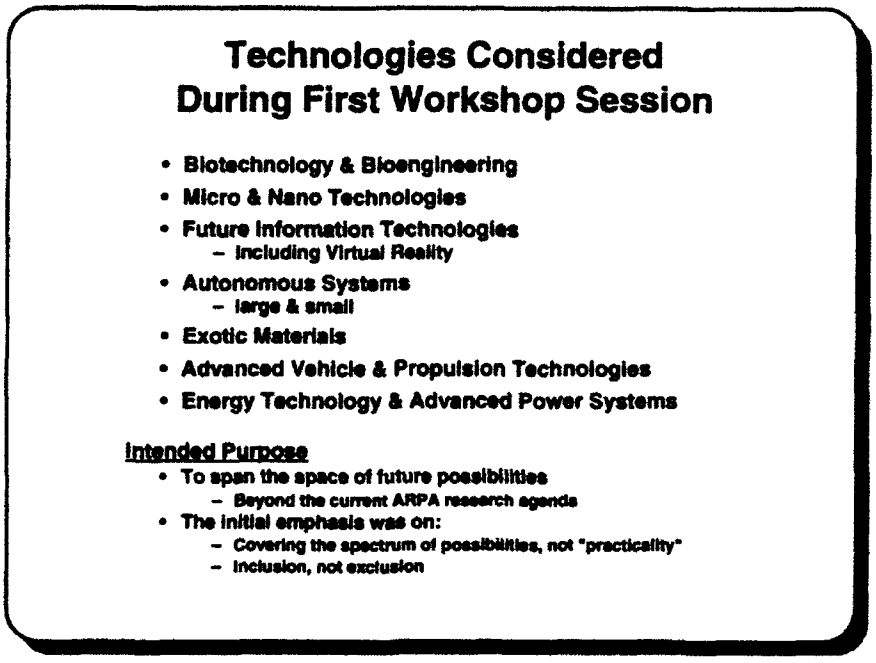
	First Session (Oct. 21-23)	Second Session (Dec. 14-16)
RAND Staff	40	38
– Military systems & operations experts		
– Technology experts		
Technology Consultants	18	14
– With expertise in specific technology areas		
RAND Military Fellows	12	8
– Air Force, Army & Navy		
Additional Consultants & Other Participants	4	6
– With expertise in:		
• Political / military environments		
• Military systems & operations		
Total	74	66

The workshop participants came from both the technology and military applications communities, and from both inside and outside of RAND. The RAND participants included researchers expert in military systems and operations, technology experts, and a number of the Air Force, Army, and Navy officers stationed at RAND as research fellows. These in-house participants were augmented by a number of consultants in relevant technology areas from both the academic and industrial research communities, and by a number of other consultants with expertise in post–cold war political and military environments and military operations. In total, 93 people participated in the workshop.[3]

These participants brought a broad and diverse mixture of talents to the workshop, covering a wide spectrum of technology areas and all facets of military operations, and including a broad perspective on strategy/policy issues in the post–cold war era. This eclectic mixture of talents was one of the strengths of the workshop.

---

[3]Appendix A lists the workshop participants.

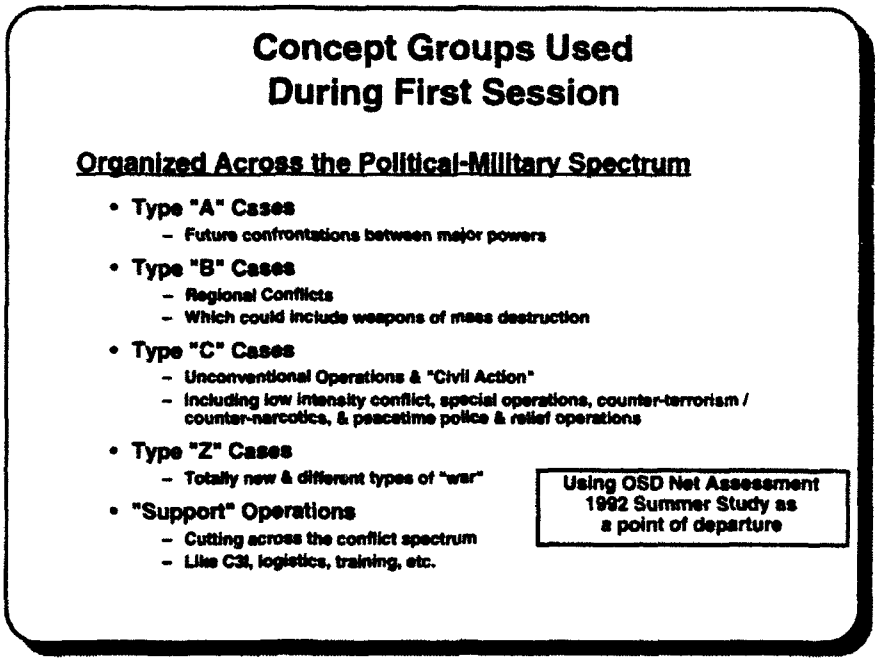


Seven technology areas, selected in consultation with ARPA, were considered during the first workshop session:

- Biotechnology and bioengineering
- Micro and nano technologies
- Future information technologies (including virtual reality)
- Autonomous systems (both large and small)
- Exotic materials
- Advanced energy and power technologies
- Advanced vehicle and propulsion technologies

The intent of this technology menu was to span the likely future "revolutionary" possibilities—beyond the current ARPA research agenda. The initial emphasis, at least in the first workshop session, was on covering the spectrum of future possibilities, not on practicality; on inclusion, not exclusion.

Technology tutorials were prepared in each of these seven areas, with the assistance of the outside technology consultants, and presented to all of the workshop participants—military applications experts as well as technologists—at the beginning of the first workshop session, to stimulate their creative imaginations.



The workshop participants then split into a number of "concept groups": mixtures of technologists and military applications experts, organized along military operations lines, across the political-military spectrum of expected future conflicts. Each of these concept groups was asked to create new application metaphors arising from the seven technologies considered in the workshop (singly or in combination), in their assigned area of military operations.[4]

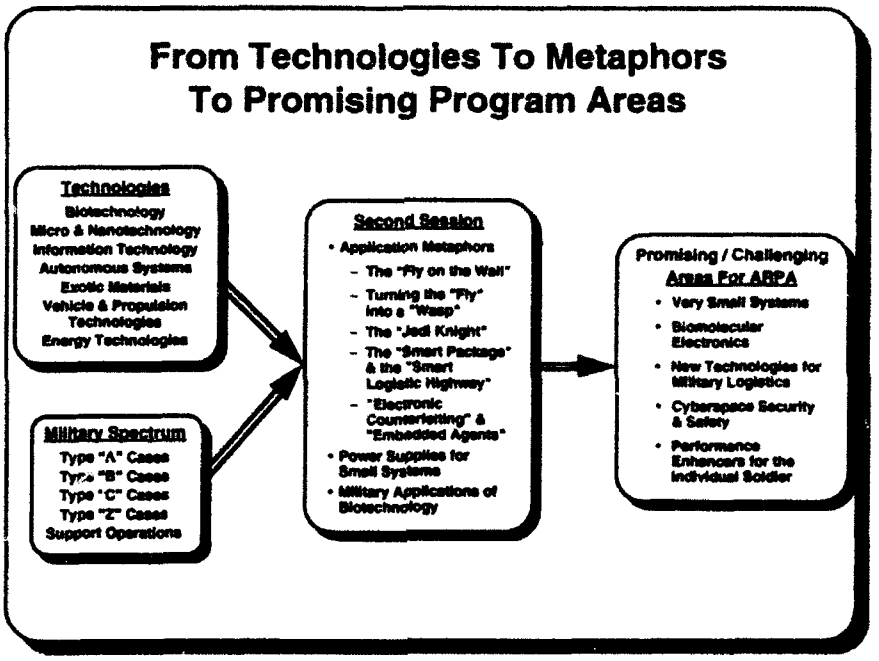
This chart lists the five concept groups used during the first workshop session. The idea for the first three of these—Type A, B, and C Cases—comes from a 1992 summer study conducted by the OSD Office of Net Assessment.[5] These three cases were intended by the participants in that study to span future conflicts.[6] We added two more concept groups for the ARPA workshop: one on Type Z Cases, totally new and different types of conflict; and one on Support Operations that cut across the conflict spectrum.

---

[4]At this stage in the workshop process, these application metaphors can be thought of as "cartoons" conveying the basic sense of a new concept, used to stimulate and focus people's imaginations.

[5]Mr. Thomas J. Welch, Associate Director of S&T, Office of Net Assessment, OSD, kindly provided us with information on the 1992 Net Assessment summer study.

[6]In the post–cold war world, terms such as "strategic war" and "tactical war"—to say nothing of "land warfare," "air warfare," and "naval warfare"—have apparently fallen out of favor as organizing categories. Hence the A, B and C cases.



This chart outlines the rest of the workshop process. The interaction of the seven technology areas and the five concept groups during the first workshop session led to the creation of a number of new application metaphors. Five of these were selected for more in-depth consideration:

- The "Fly on the Wall"
  - Miniature fly-sized vehicles carrying a variety of sensors, for unobtrusive surveillance in a variety of military situations.
- Turning the "Fly" into a "Wasp"
  - Micro systems that disable enemy systems. A "Fly with a stinger."
- The "Jedi Knight"
  - Multiple performance enhancements for the individual soldier.
- The "Smart Package" and the "Smart Logistic Highway"
  - New ways of conducting military logistics.
- "Electronic Counterfeiting" and "Embedded Agents"
  - Counterfeiting of electronic information of all kinds.
  - Hardware and software "agents" embedded in a variety of information systems.

During the second session, working groups attempted to flesh out each of these five metaphors, sketching out system concepts and their possible impacts, and identifying the system performance and technology thresholds required for truly revolutionary impacts on military operations.

Since several of these metaphors involved very small—indeed, tiny—systems, another working group looked into the technical possibilities for power supplies for such systems. Still another group considered military applications of biotechnology, a subject that had raised much interest, but little closure, during the first session.

By means of this process, we identified four promising program areas as candidates for new ARPA research initiatives:

- Very small systems
  - The use of micro and nano technologies to develop miniature (e.g., fly-size) flying and/or crawling systems capable of performing a wide variety of battlefield sensor missions.
- Biomolecular electronics
  - The use of techniques from molecular biology and biotechnology to develop new molecular electronic materials, components, and computational architectures.
- New technologies for military logistics
  - The use of modern microelectronic and information technologies as the basis for a new advanced-technology military logistic system.
- Cyberspace security and safety
  - The development of techniques and strategies to protect U.S. interests in and relating to "cyberspace"—the global world of internetted computers and communication systems in which more and more U.S. activities (military and civilian, governmental and nongovernmental, economic and social) are being carried out.

The first three of these represent technological opportunities for ARPA. The fourth is an emerging national problem area in which ARPA could play an important role.

Finally, we also identified a fifth program area as a promising candidate for enhanced ARPA research efforts:

- Performance enhancers for the individual soldier
  - The use of a variety of technologies to enhance the survivability, mobility, and mission performance of individual soldiers.

From Program Areas Back To Applications

Candidate Program Areas	Conflict Spectrum: Type A Conflicts Between Major Powers	Type B Regional Conflicts	Type C Low-Intensity Conflicts & Special Ops.	Type Z Totally New Types of "War"
Very Small Systems	(X)	X	X	
Biomolecular Electronics	X	X	X	
New Technologies for Military Logistics	X	X	X	
Cyberspace Security & Safety	(X)	(X)	(X)	X
Performance Enhancers for the Individual Soldier	(X)	(X)	X	

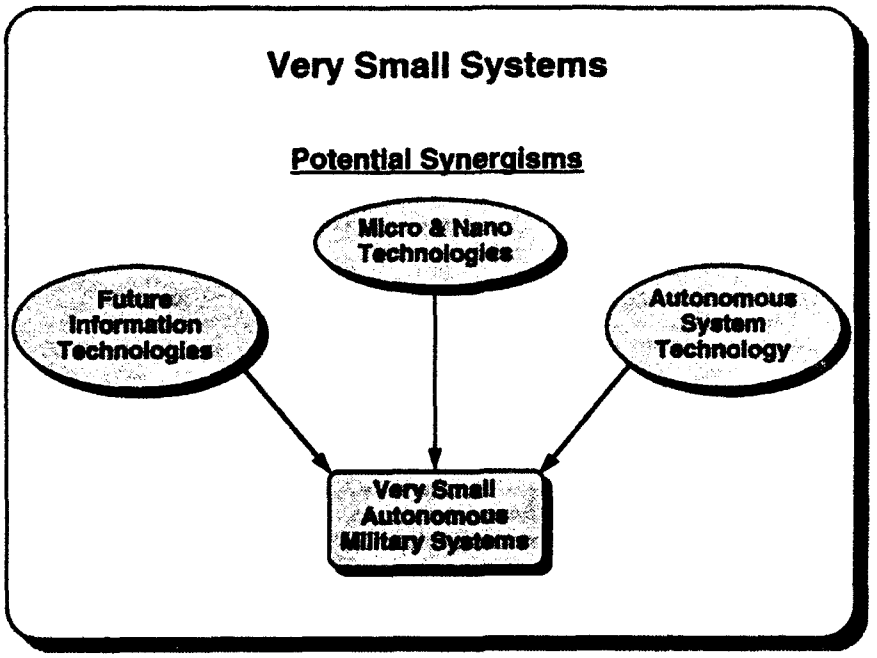
As we have described, the five candidate program areas arose out of the application metaphors, which in turn arose out of the workshop interactions between the various technology areas and the different concept groups spanning the spectrum of future conflicts. Looking backwards, from the program areas to the conflict spectrum, this chart indicates where in the spectrum of future conflicts we expect each of these five program areas to contribute.

As the chart shows, we expect that the very small systems program area will lead to a variety of applications useful in Type B (regional conflicts) and Type C (low-intensity conflict and special operations conflicts), with possible applications also to Type A (conflicts between major powers). Both the biomolecular electronics and new technologies for military logistics program areas should lead to applications useful across the entire spectrum of Type A, B, and C conflicts. The cyberspace security and safety program area is motivated primarily by consideration of Type Z (totally new types of "war") conflicts, but should also have applications across the spectrum of Type A, B, and C conflicts. The performance enhancers for the individual soldier program area is motivated primarily by consideration of Type C conflicts and should find its primary applications there; it is likely also to lead to applications useful in Type B conflicts, and perhaps in Type A conflicts as well.

We now turn to a discussion of the five candidate program areas.

2. Very Small Systems

We begin with very small systems.



The opportunities in the very-small-systems area arise as a result of emerging synergisms between three technologies:

- Micro and nano technologies[7]
- Future information technologies
- Autonomous system technology

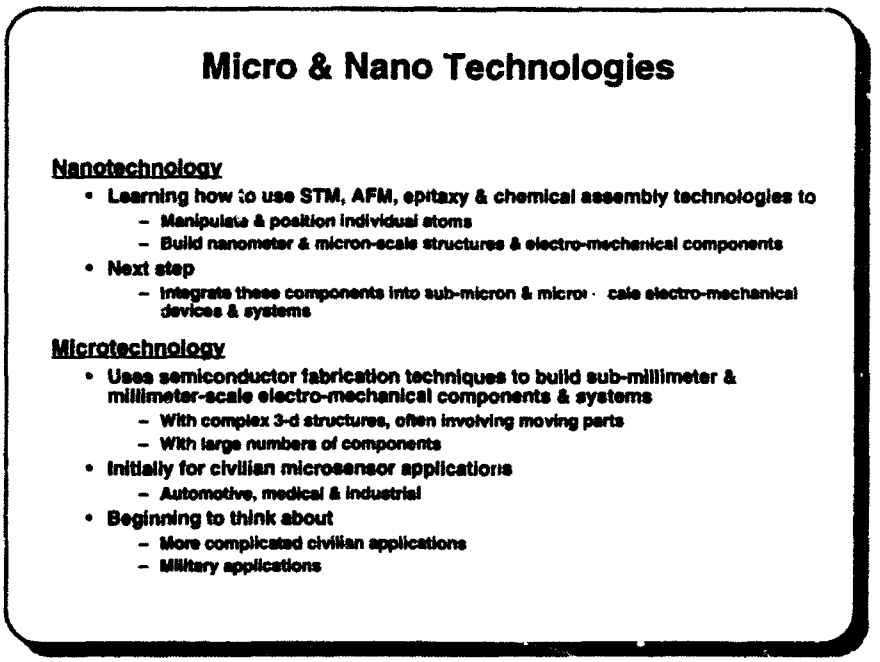
which in combination raise the prospect of *very small autonomous systems.*[8]

We begin by briefly reviewing the state of the art of each of these technologies.

---

[7]As used here, "micro" refers to structures and components and systems ranging in size from one micron (10^{-6} meter) to one millimeter (10^{-3} meter). "Nano" refers to structures and components and systems ranging in size from one nanometer (10^{-9} meter) to one micron (10^{-6} meter).

[8]These prospects are further enhanced by developments in energy technologies and in advanced materials.



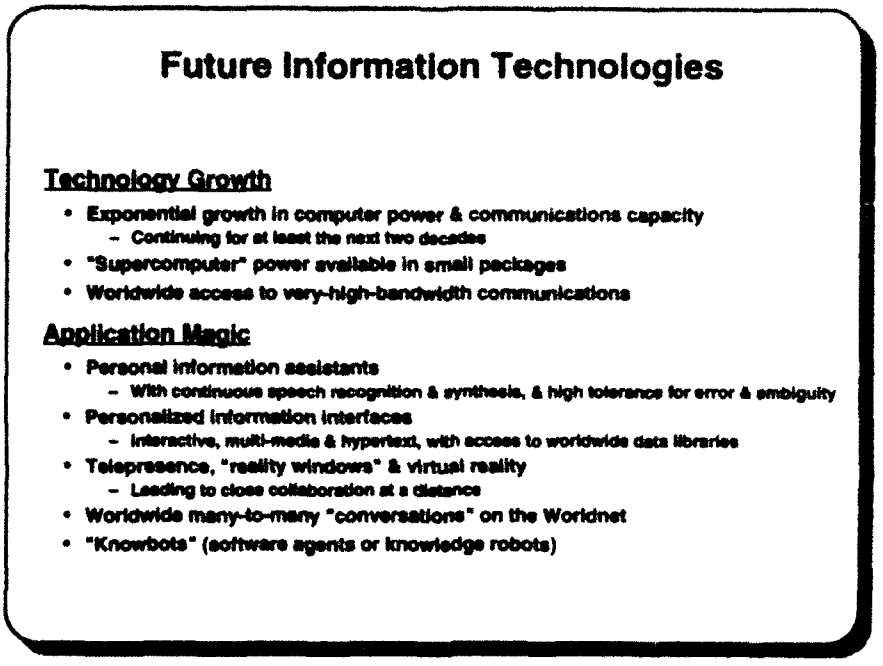
In the nano technology area, scientists have recently learned to use the scanning tunneling microscope (STM), the atomic force microscope (AFM), epitaxy, and chemical assembly technologies to manipulate and position individual atoms, and to build nanometer and micron-scale structures and electro-mechanical components.[9] The next step, which nano technologists are beginning to think about, will be to integrate these components into submicron and micron-scale electro-mechanical devices and systems.

In the micro technology area, things are already further along. Scientists have used semiconductor fabrication techniques to build sub-millimeter and millimeter-scale electromechanical components and systems. Many of these microelectromechanical systems (MEMS) have complex three-dimensional structures, with large numbers of components and, often, moving parts. Thus far, most of these MEMS developments have been for civilian microsensor applications, particularly in the automotive, medical, and industrial arenas. However, people are beginning to think about more complicated civilian applications that go beyond a purely sensor function, and about military applications.[10]

---

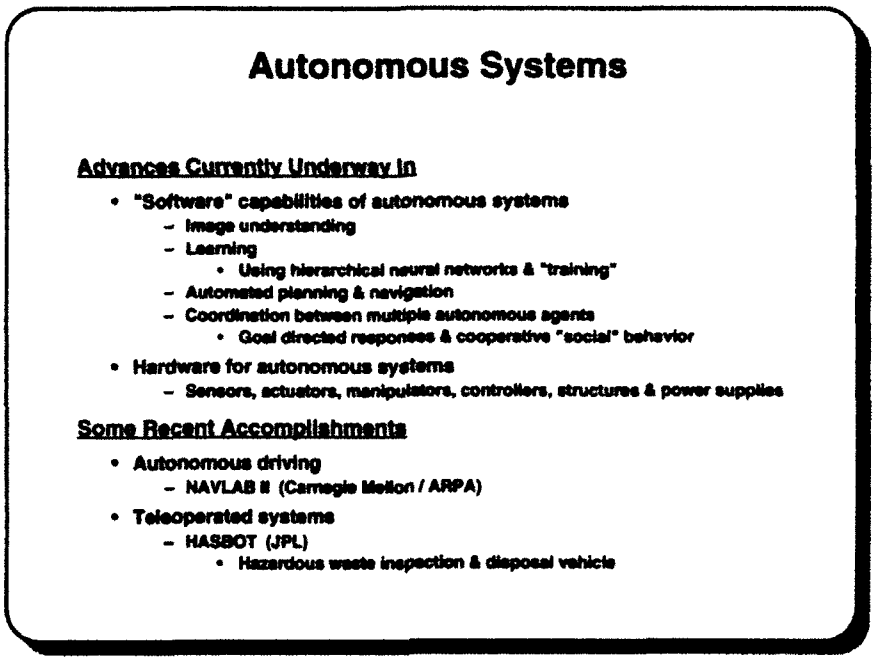
[9]Recent advances in nano technology are discussed in Gardner and Hingle (1991), Whitehouse and Kawata (1990), MacDonald (1992), Whitesides et al. (1991), and Cho (1988). Feynman had a prescient view of this subject in 1959, see Feynman (1959); it is still worthwhile reading today.

[10]Brendley and Steeb (1993) review recent developments in micro-electromechanical systems.



Everyone is conscious of the enormous strides that information technology has made over the last several years. The best expert opinion is that this exponential growth in computing power and communications capacity will continue for some time to come. In the not too distant future, this will lead to "supercomputer" capabilities in small packages, the so-called supercomputer on a desktop, and to very impressive computer capabilities, if not at the supercomputer level, in very small—even tiny—packages. These computing capabilities will be available to almost everyone, along with worldwide access to very-high-bandwidth communications (i.e., gigabits/sec or more).

This continued growth in information technology will make possible even more application "magic," to change the way we work and the way we live. A few examples of possible future applications of information technology are listed on the chart, but these are just the ideas that people are discussing today. The most "magical" applications probably haven't been thought of yet.



Major advances are also under way in the technology of autonomous systems. Improvements are being made in all of the hardware components going into autonomous systems: sensors, actuators, manipulators, controllers, structures, and power supplies. At the same time, and perhaps even more important, striking progress is being made in the "software" capabilities of autonomous systems. This includes areas such as:

- Image understanding
  - The ability of an autonomous system to process and "understand" in a useful fashion the scene that its sensors see.
- Learning
  - The ability of an autonomous system to learn to do a task, as a result of a series of training or teaching experiences.
- Automated planning and navigation
  - Automated capabilities to plan a "mission" for an autonomous system to perform, and to chart a course for such a system to follow.
- Coordination between multiple autonomous agents
  - The beginnings of cooperative "social" behavior in autonomous systems.

The workshop reviewed a number of recent accomplishments in autonomous system technology that illustrate these hardware and software advances. One of the most interesting and instructive examples presented was the NAVLAB II autonomous driving system being developed by Carnegie Mellon, under ARPA sponsorship. This system, mounted on a HMMWV (wheeled) vehicle and including forward-looking TV and imaging long-wavelength infrared (LWIR) sensors, as well as a laser range finder, has demonstrated fully autonomous (i.e., with essentially no intervention by a human driver) driving in the following situations:

- On a freeway in the midst of other traffic, at speeds of up to 55 mph, for distances of up to 22 miles.[11]
- Cross country, over a variety of terrains, at speeds of 8 mph, for distances of up to 2 miles.

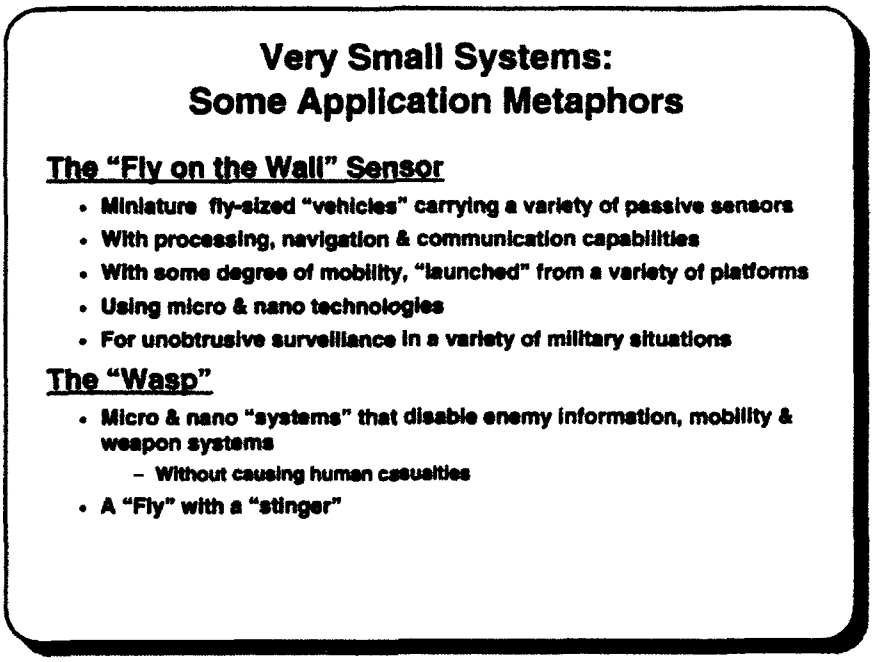
One of the keys to the NAVLAB II accomplishments is the use of a set of hierarchical neural networks, as the "brains" of the system. These neural networks are trained by "watching" a human driver steer the vehicle in a representative set of situations.[12]

Compared with what the best autonomous systems could do 10 years ago, the performance of NAVLAB II is truly magical.

---

[11]These were the late-1992 performance numbers. More recently, NAVLAB II has extended its freeway driving to distances of 90 miles. It still has some things to learn about driving on freeways, however: in particular, how to handle off-ramps. NAVLAB II doesn't know how to ignore off-ramps. It takes every one it sees, unless a human monitor intervenes.

[12]In the initial training, the human driver never made mistakes (never veered toward the side of the road, never got too close to another vehicle, etc.), so the neural networks never learned how to take corrective actions in adverse situations. To properly train the networks for all of the situations they might encounter, the human drivers had to deliberately make mistakes, so the neural networks could "watch" their corrective actions.



Putting together these three technologies—micro and nano technology, future information technology, and autonomous system technology—suggests a new possibility: very small, even tiny, autonomous systems. Thinking about things that such systems could do led the workshop to two application metaphors: the "Fly on the Wall" sensor, and the "Wasp."

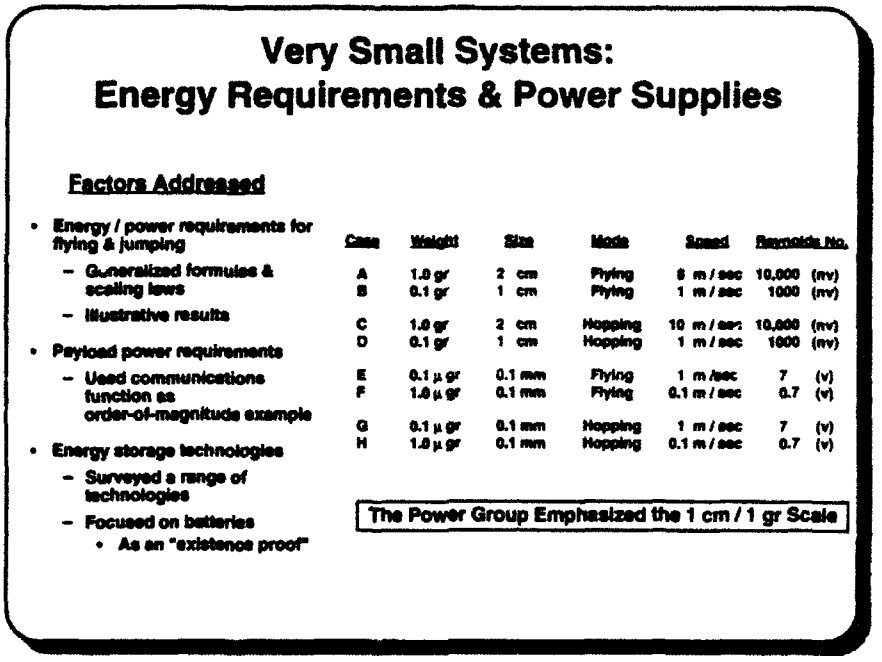
The "Fly on the Wall" is envisaged as a miniature, fly-sized vehicle carrying a variety of passive sensors. It would have processing, navigation, and communication capabilities.[13] It would have some degree of mobility—flying, crawling, hopping, etc.—and could be launched from a variety of platforms. It would be used for unobtrusive surveillance in a variety of military situations. The "Fly on the Wall" would be built using micro and nano technologies, which presumably would permit inexpensive fabrication of large numbers of "Flies."

The "Wasp" is a micro/nano system that disables enemy information, mobility, and weapon systems without causing human casualties. The "Wasp"can be thought of as "Fly" with a "stinger."

The second workshop session looked at both of these metaphors.

---

[13]The navigation suite would include a miniature Global Positioning System (GPS) receiver.



One of our first concerns was energy: Would one of these very small systems be able to carry enough stored energy on its mission to go a useful distance? To perform a useful set of functions? Or would energy considerations make it virtually immobile , tied to the nearest "wall plug"? In other words, how far can we expect our "Fly" to fly on its own? Across the room, or across the city?

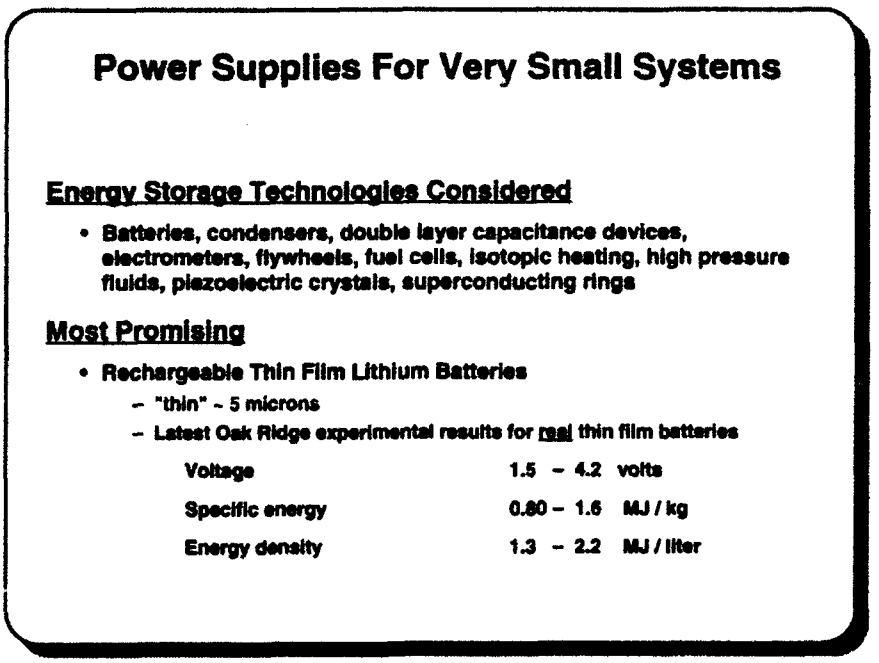
During the second workshop session, a working group including experts on advanced energy storage technologies and on the locomotion of micro-vehicles looked into this question. As this chart indicates, they considered the energy and power requirements for micro-flying and micro-jumping (i.e., hopping).[14] They also briefly addressed payload power requirements, using the communications function as an order-of-magnitude example.

In their investigations of micro-locomotion, the group discussed both flying and hopping, and initially considered the entire weight/size/speed range shown on the chart. This covers a wide range of Reynolds numbers, from the nonviscous regime down to the viscous regime.[15] For their final, detailed calculations, they emphasized the upper end of this range, the 1 centimeter/1 gram scale.

---

[14]Two recent papers on micro-locomotion are Solem (1991) and Crary et al. (1992).

[15]Solem (1991) discusses how micro-flight changes as one moves from the nonviscous to the viscous regime.



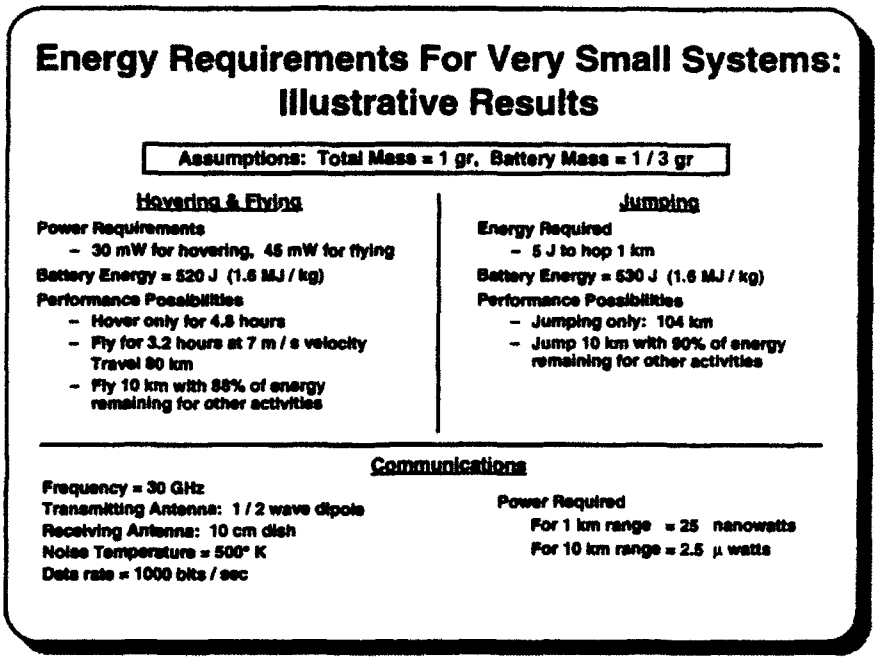
A wide range of energy storage technologies were considered for micro-vehicles, including all of those shown on this chart. From these, batteries—particularly rechargeable thin film lithium batteries—were selected as currently the most promising for micro-vehicle applications.[16]

The values shown on the chart for the voltage, specific energy, and energy density of such batteries are based on recent experimental results at Oak Ridge National Laboratory.[17]

---

[16]This is probably not a definitive judgment, true for all time. Other energy storage technologies may ultimately turn out to be competitive for micro-vehicles. The results shown on the next chart, for micro-locomotion using rechargeable thin film lithium batteries, should be thought of merely as an "existence proof" that such locomotion is feasible over useful ranges.

[17]Dr. John Bates, Oak Ridge National Laboratory, provided these data.



Using this battery technology, the energetics of a conceptual micro-vehicle with a length of 1 centimeter and a total mass of 1 gram were considered. Based on order-of-magnitude calculations carried out during the workshop,[18] such a vehicle would require:

- 30 milliwatts for hovering
- 45 milliwatts for flying
- 5 joules to hop 1 kilometer.

Assuming that one-third of the total vehicle weight was the battery, using the Oak Ridge rechargeable thin film lithium battery technology with 1.6 MJ/kg, the total stored battery energy would be 530 joules. This would permit:

- Hovering for 4.9 hours
- Or flying for 3.3 hours at a speed of 7 meters/sec, covering 80 kilometers
- Or flying for 10 kilometers, with 88% of the stored energy remaining for other activities
- Or jumping for 104 kilometers
- Or jumping for 10 kilometers, with 91% of the stored energy remaining for other activities.

[18]These calculations are summarized in Appendix B.

The power required for an illustrative communications situation was also estimated. The micro-vehicle was assumed to transmit at 30 GHz to a nearby "mother" vehicle, using a 1/2-wave dipole antenna. The mother vehicle, which can be larger, was assumed to have a 10 centimeter diameter dish as a receiving antenna. Assuming a data rate of 1000 bits/sec, the power required for communications is:

- 25 nanowatts for a 1 kilometer range
- 2.5 microwatts for a 10 kilometer range.

Both of these values are much smaller than the power required for locomotion. Other payload functions (passive sensing, navigation and control, etc.) are likely to require power levels of about the same order of magnitude as communications.[19] Accordingly, it appears that locomotion will dominate the energy requirements for micro-vehicles, and that current state-of-the-art miniature battery technology will support useful vehicle ranges of at least 10 kilometers.

These were not definitive design calculations. They should be regarded merely as an existence proof that micro-vehicles with militarily useful ranges are energetically feasible.

---

[19]The exception to this would be active sensors, such as a miniature active radar or a laser. We have not estimated the power requirements for such active sensors.

The "Fly on the Wall": Some Sensor Candidates

Sensor Category	Range from Source: Contact	Near (meters)	Intermediate (10 – 100 m)	Far (100 m – 1 km)	Distant (≥ 1 km)
Acoustic		Personnel	Vehicles	Helicopters	
Seismic		Vehicles, Personnel			
Visible		← Useful Imaging →			
Imaging IR		← Useful Imaging →			
Non-Imaging IR	Local Temperature				
Magnetic			Vehicles		
Chemical		Vehicle Exhaust	Dispersed Chem Agents →		
Biological			Biological Agents →		
Gamma Ray		Nuclear Weapons			

Work is currently under way in the United States on a number of micro-sensors that are potentially suitable for use on tiny vehicles. There is research on:

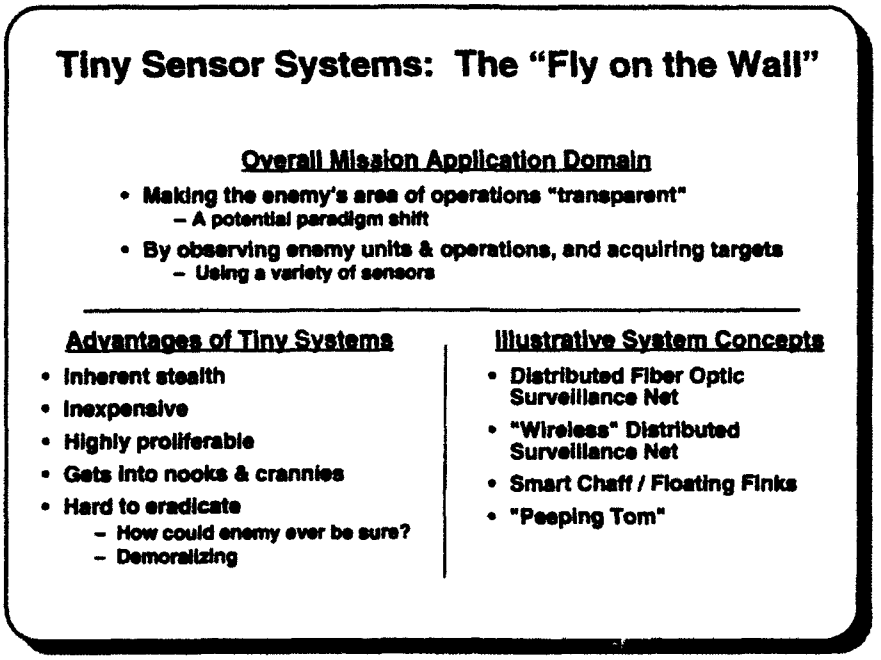
- Acoustic sensors using piezoelectric diaphragms
- Miniature resonant-beam accelerometers that could be used as seismic sensors[20]
- Infrared sensors, including
  - pyroelectric or semiconductor thin-film arrays (imaging)
  - gas cell bolometers (non-imaging)
- Visible imaging sensors using charge-coupled device (CCD) arrays
- Magnetic sensors using
  - thin-film magnetoresistive detectors
  - intergrated-circuit-technology-based Lorentz-force devices
- Chemical sensors, including
  - Pt-gate MOSFET chemiresistors
  - resonant beam devices

[20]This technology is driven by applications in the automotive industry. The first application envisaged is crash detection. Additional, future applications include dynamic suspension, skid detection for anti-lock brakes, and inertial navigation systems.

- Biosensors
- Gamma-ray sensors using high-Z semiconductor detectors.

Almost all current micro-sensor research is focused on commercial applications, mostly at very short ranges—in contact or near contact with the source of the phenomena they are sensing. Based on what has been accomplished thus far in these commercial endeavors, and researchers' estimates of what might be accomplished in these micro-sensor technologies over the next five to ten years, the chart on the previous page provides order-of-magnitude estimates of the ranges at which such micro-sensors might detect various types of military targets, if they were employed in such applications.

As can be seen from the chart, depending on the nature, size, and signature of the military target, such micro-sensors might provide detection ranges from the very short (a few meters or less) to the reasonably long (100 meters or more).



The previous discussion offers the prospect that:

- Tiny micro-vehicles can be built.
- They can carry enough stored energy to travel militarily useful distances.
- They can carry sensors capable of useful detection ranges against a variety of military targets.

This engineering prospect leads to a large number of specific military application concepts. These concepts all coalesce into one broad, overall mission application domain:

- Making the enemy's area of operations "transparent"
  - By observing enemy units and operations, and acquiring targets, using a variety of sensors.

As the chart indicates, this could lead to a potential "paradigm shift" in military operation—a true revolution in military operations.

As currently conceived, these tiny "Fly on the Wall" sensor systems would have several inherent advantages:

- They would be inherently stealthy.
- They are assumed to be inexpensive to fabricate, and therefore highly proliferable. One could employ hundreds or thousands of "Flies" in an operation, not just a few.

- They would be very hard for the enemy to eradicate, because of their small size and their large numbers, and because they could get into nooks and crannies. The opponent would never be sure that he had gotten rid of them all, which could be demoralizing.

During the second workshop session, we identified a large number of concepts for such "Fly" systems. One feature of many of these concepts was a hierarchy of vehicles:

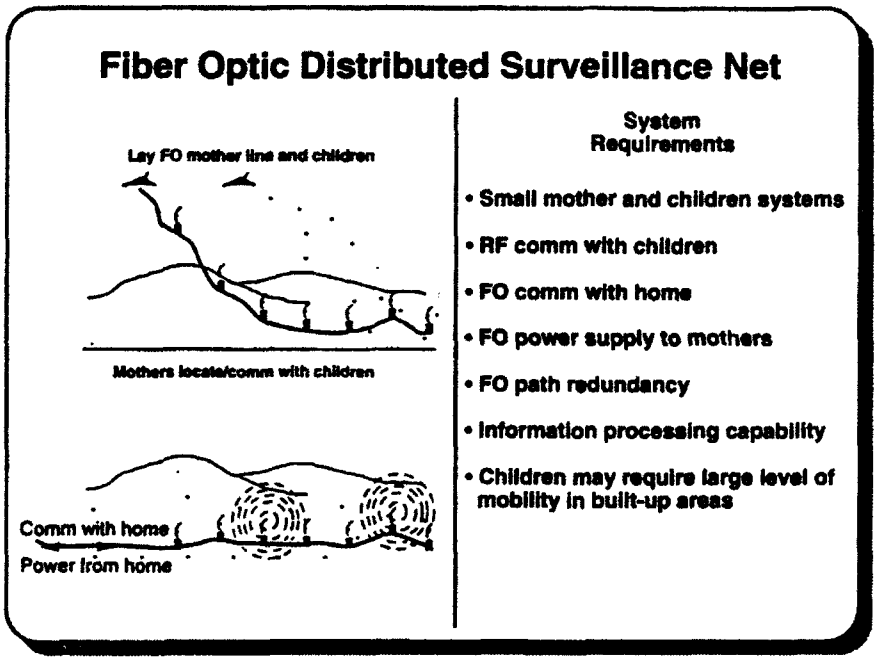
- "Children"—micro-vehicles that carry the sensors, have mobility over a limited range, and can communicate over a limited range.
- "Mothers"—a smaller number of larger vehicles that carry the "children" to the immediate vicinity of the operational area, release them, act as communications relays, and, if necessary, collect the children after the operation.[21]

This "mother" and "children" hierarchy may turn out to be a general feature of practical micro-vehicle system concepts.

The next four charts present four of the system concepts identified during the workshop as illustrative conceptual examples of a much larger set.

---

[21]It is an open question whether the micro-vehicles should be considered "throw-aways" or should be recovered and reused. The answer will depend on their fabrication costs (including structure, propulsion, navigation, control and communications systems, and the miniature sensor payloads) compared to the cost and complexity of recovery operations.

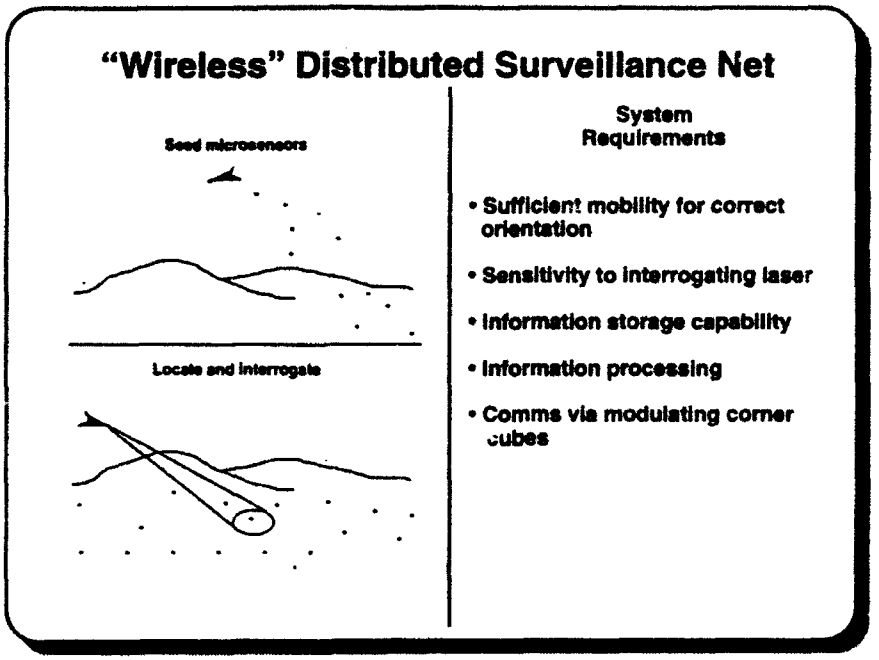


In this concept, called a "Fiber Optic Distributed Surveillance Net," aircraft or helicopters lay down one or more fiber-optic lines, each containing a number of "mother" nodes. The aircraft also disperse a much larger number of "children." The children act as the sensor front-ends on a distributed surveillance net.

There is radio frequency communications between each mother and its nearby children. The mothers in turn communicate via the fiber-optic lines with some kind of "home." The fiber-optic lines also provide power to the mothers.

Between them, the mothers and children can have a considerable degree of information processing capability, which can be used, among other things, to distinguish targets from background and to localize targets. How this processing capability is divided between mothers and children can vary, depending on the details of the operational concept and system design.

Such a distributed surveillance net can perform a number of battlefield surveillance missions at various depths within the enemy's area of operations, and utilizing a variety of sensors. Depending upon the details of the specific application, the children vehicles may require more or less mobility.



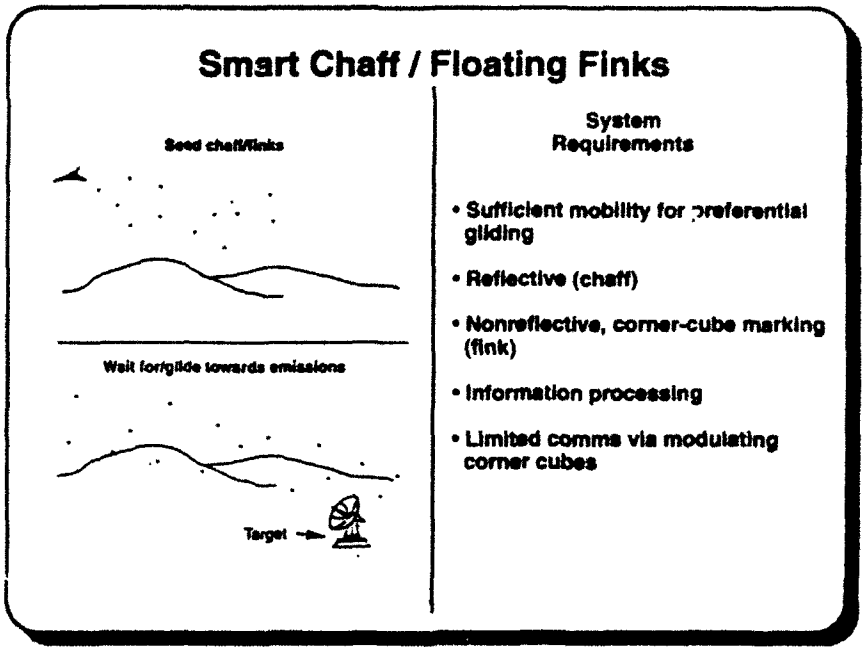
In the "Wireless" Distributed Surveillance Net concept, an aircraft or helicopter disperses a large number of micro-sensor vehicles. These micro-vehicles drift down to the ground. They have sufficient mobility to orient themselves on the ground (e.g., to get the right end up and pointed in the proper direction), and perhaps to move around a bit (e.g., to get out from behind an obstruction), but they do not require a large degree of mobility.

These micro-sensor vehicles act as a "wireless" distributed surveillance net. Overflying aircraft or helicopters interrogate the sensor-net area with lasers. The micro-sensor vehicles carry corner cubes that retroreflect the laser radiation back to the aircraft or helicopter. By modulating the corner cubes, sensor data are transmitted back to the interrogating vehicle.

Each micro-sensor vehicle has its own information processing capability. This is used for a variety of tasks, including the discrimination of targets from background.

Much the same as the fiber-optic distributed surveillance net, the wireless distributed surveillance net can perform a number of battlefield surveillance missions, at various depths within the enemy's area of operations and utilizing a variety of sensors. Whether the fiber-optic or the wireless version proves to be better will depend on the details of the specific application.

In this concept, as well as the next one, there is no "mother" vehicle per se—other than the aircraft or helicopter.

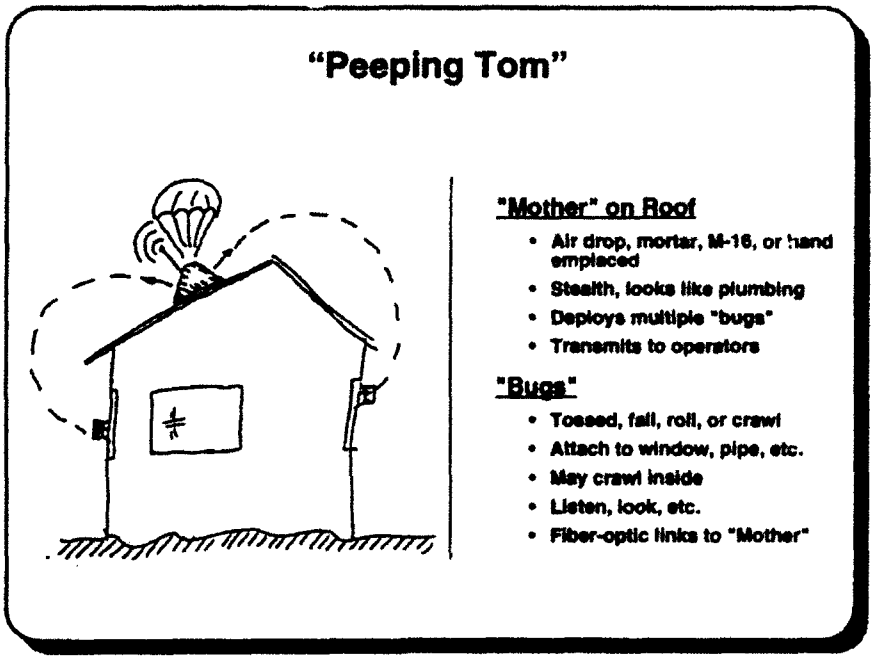


In the "Smart Chaff" or "Floating Finks" concept, an aircraft or helicopter once again disperses a number of flying, or at least gliding, micro-vehicles. These vehicles have sufficient mobility to "hang" in the air until they sense electromagnetic emissions from a radar or a radio transmitter. They then glide down to that emitter, and alight on it or near by.

After landing, they can do one of two things:

- Wait to be interrogated by a scanning laser, at which time they use retroreflecting corner cubes to report back the presence and location of the emitter (even if the emitter has turned itself off).
- Actively transmit the presence and location of the emitter, for as long as their energy supply lasts.

These micro-vehicles will also have an onboard information processing capability. Among the functions it can perform is the identification of emitter type.



In the "Peeping Tom" concept, a "mother" vehicle is placed on the roof of a building believed to contain enemy personnel, equipment, etc. This placement can be accomplished in a variety of ways: an air drop, a mortar or M-16 round, hand emplacement, etc. This mother vehicle is "stealthy": it is designed to have the external appearance of something that might naturally occur on the roof of a building (e.g., plumbing, a bird or insect nest, etc.).

Once in place on the roof, the mother deploys a number of miniature "bugs" carrying a variety of sensors. These bugs hop, crawl, roll, and/or fall down, around, and into (if the building has any openings) the building. (If they cannot get inside, these bugs could attach themselves to the outside of windows.)

Once in position, the bugs listen, look, smell, etc., and report back to the mother what they sense, via fiber-optic links. The mother in turn transmits the sensor data back to the operators of the system.

As in the previous concepts, this system will have some degree of information processing capability, divided between the mother and the bugs.

There are obviously a large number of "eavesdropping" or surveillance missions that such a system could perform—on the battlefield as well as in other situations.

These four illustrative systems merely sketch out the "space" of possible micro-vehicle application concepts. They in no way exhaust it. There are hundreds of other interesting ideas.

The "Fly on the Wall": Some Key Challenges

- **To be affordable in large numbers**
  - **Not just inexpensive in small numbers**
- **Management of complex surveillance networks**
  - **Involving hundreds or thousands of sensors**
- **Efficient operational emplacement**

The previous four examples are illustrative of the wide variety of ways in which the "Fly on the Wall" concept could be realized and suggestive of the wide variety of battle surveillance missions to which such systems could be applied. There are a number of key challenges that must be overcome to realize the mission potential suggested by these examples. Three of the most important, beyond the obvious technical challenges associated with building the individual "Flies," are:

- *Making the Flies truly affordable in large numbers.* Most, if not all, of the application concepts envisaged assume the employment of hundreds or thousands of Flies in an operation, not just a few. These large numbers of Flies are necessary both to cover a large enough area of the battlefield, given the relatively short sensor range of each individual Fly, and to make the enemy's job of eradicating them inherently difficult. This means that the individual Flies must be extremely inexpensive to fabricate, like microcircuits that can be proliferated in large numbers, and not hand-made, carefully tuned "Swiss watches." Realizing this in practice will be a major technical challenge.
- *Managing complex surveillance networks.* This could require the collection and correlation of reports from hundreds or thousands of sensors, each of which covers only a small part of the total area of interest and many of which may be imprecisely located. Ways must be developed to efficiently and effectively process the data from

such a network.[22] This will be both a technical and operational challenge.

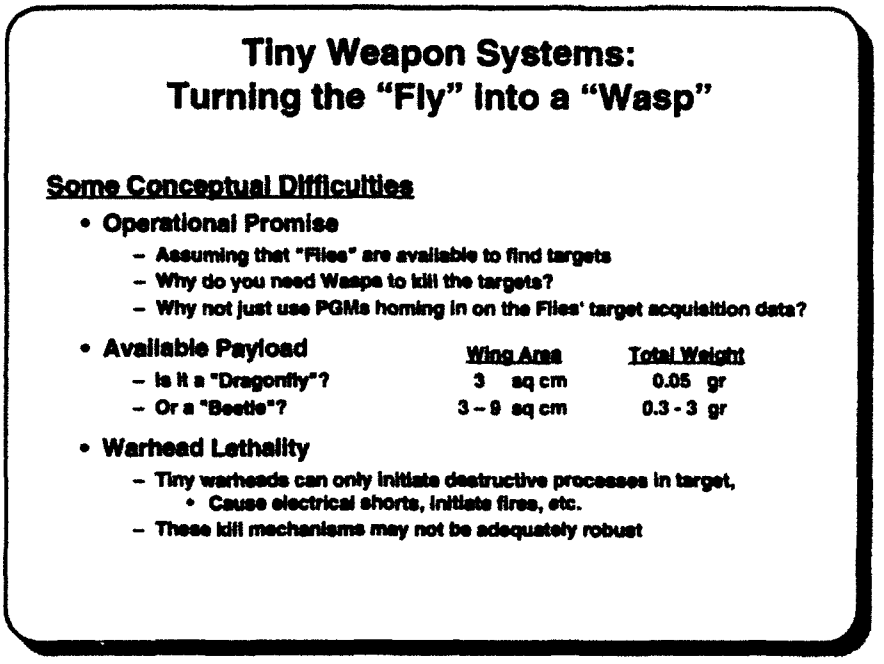
- *Efficient operational emplacement.* The emplacement process must distribute the individual Flies efficiently across the area to be covered, with most of them in productive surveillance positions, while ideally ensuring the survivability of the emplacer and not tipping off the enemy regarding the presence of the surveillance net. Further, the emplacement process should be robust with regard to environmental variables (e.g., weather, winds). This will also be both a technical and operational challenge.[23]

These are key challenges—there are undoubtedly others as well—that the workshop could only identify and not address in detail.

---

[22]The processing techniques developed and applied in previous unattended-ground-sensor programs could be a useful point of departure here.

[23]Here again, deployment techniques developed and applied in previous unattended-ground-sensor programs could be a useful point of departure.



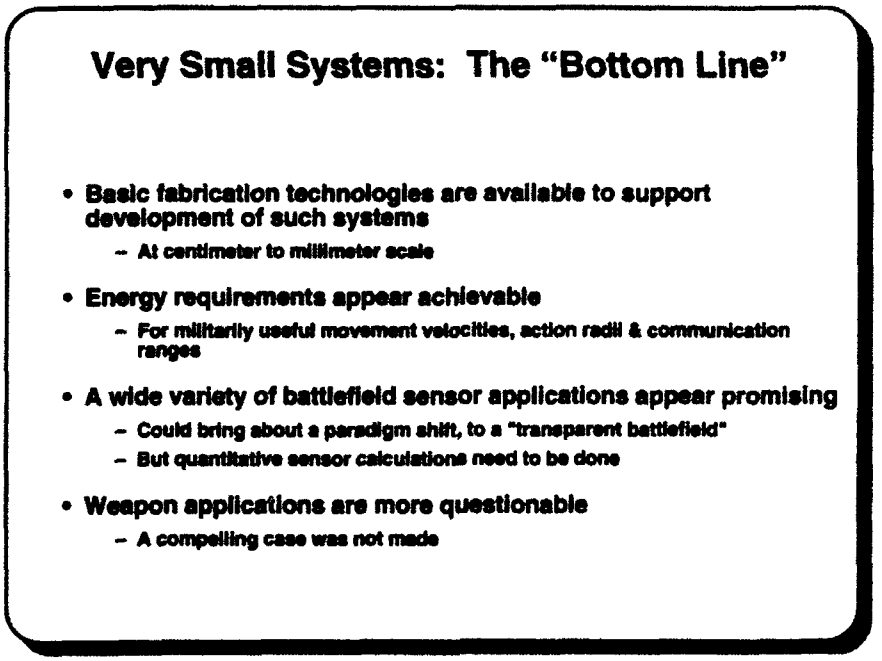
In addition to looking at the "Fly on the Wall," fly-sized micro-vehicles performing sensor missions, the workshop also looked at another metaphor, the "Wasp": micro-vehicles that carry some sort of a tiny warhead, a "stinger," that could cause damage to some types of military systems.

Our discussions of this application metaphor were not as promising as those of the "Fly." We ran into three conceptual difficulties:

- Lack of compelling operational promise.
  - Assuming the Flies are available to find targets, why are Wasps needed to kill the targets? Why not just use precision-guided munitions (PGMs) homing in on the target acquisition data (e.g., GPS coordinates) provided by the Flies? This should give a much higher-confidence kill.
- Uncertainties concerning the size of micro-payload available for a warhead on a Wasp.
  - In the insect realm, on which many of the current micro-vehicle design estimates are based, insects of similar wing area can have vastly different total weights. For example, both the dragonfly and the beetle have wing areas of a few square centimeters. But a beetle has a total weight from 10 to almost 100 times greater than that of the dragonfly. This leads to similar uncertainties in estimates of the weight available for the "stinger" on a Wasp.

- Concerns about the lethality of such miniature warheads.
  - Generally speaking, such tiny warheads cannot kill the target all by themselves. What they do instead is initiate destructive processes in the target, by causing electrical shorts or fires, for example. These kill mechanisms may not be adequately robust for high-confidence target kills.

Taken together, these three conceptual difficulties led to a considerable loss of enthusiasm for the Wasp application metaphor. Most of the workshop participants did not find it very compelling.

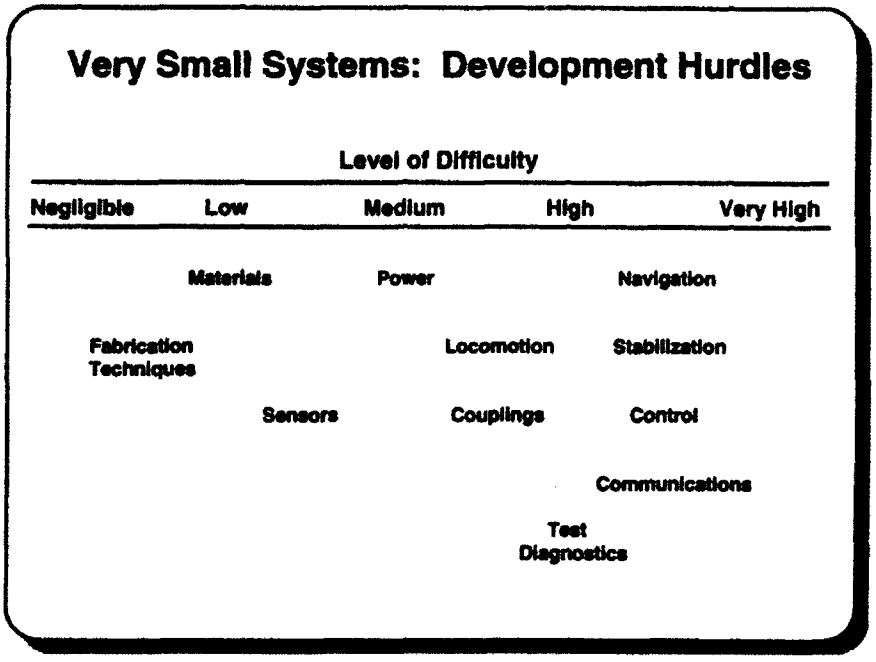


Based on these considerations, the workshop reached the following conclusions concerning very small systems:

- Basic fabrication technologies are available to support development of such systems, at the centimeter to millimeter scale.
- The energy requirements for militarily useful movement velocities, action radii, and communication ranges appear achievable.
- A wide variety of battle sensor applications appear promising.[24] These could bring about a paradigm shift in military operations, to a "transparent battlefield." This would truly be a revolution in military operations.
- Weapon applications of such tiny systems are much more questionable. A compelling case for micro-weapon systems was not made during the workshop.

---

[24]However, quantitative calculations of sensor performance need to be carried out.



The workshop took a cursory look at the development hurdles confronting very small systems. This chart summarizes our initial impressions.[25] The semi-precise meanings of the level-of-difficulty categories used on the chart are:

- Negligible
  - The capability is well established. Researchers in the field are doing similar things today.
- Low
  - This can be done using current state-of-the-art, but informed choices must be made.
- Medium
  - Researchers in the field believe they know how to do this, but it will not necessarily be easy.
- High
  - This will be hard to do, but researchers in the field have some ideas of how to attack the problem.

[25]These should be viewed as the initial judgments of experts in the area, not as the results of a detailed investigation.

- Very High
  - This will be hard to do, and today researchers do not know how to go about it.

The following comments expand on the entries in the chart on the previous page:

Fabrication Techniques At the centimeter to millimeter scale, "conventional" machining techniques (i.e., small watch scale) can be used for early prototypes. Silicon fabrication techniques should be available for production vehicles.

Materials There are no real problems here. Several choices are available.

Power The first systems should probably use thin-film batteries. Other miniaturized approaches are possible, but need more investigation.

Locomotion For *flying*, some data are available, but more checks are needed. For *jumping*, the dynamics are less studied, but the gross attributes do not appear unduly hard. For *swimming*, there is much theory available; hydrodynamic tests will require care.

Couplings For the coupling of the energy source to the motor, there is some small-scale experience. For the coupling of motor to actuator, there are limited data in a practical sense. For the details of the actuator, design studies are needed for optimization.[26]

Sensors Optical and infrared sensors are the only sensors facing intrinsic problems due to the small scale; the resolution achievable with miniature optical/IR sensors will be substantially limited by diffraction —much more so than for sensors of more normal size. The effects of noise will be important for miniature sensors of all types. At the beginning of a research program, miniature sensor technologies can be developed and tested separately from integrated locomotion systems.

Test Diagnostics This area requires a great deal of attention. Semi-quantitative "go-no go" tests will sometimes be useful, but detailed quantitative measurements will usually be required for design optimization. This will require new types of test instrumentation, which should be considered from the beginning of any program.

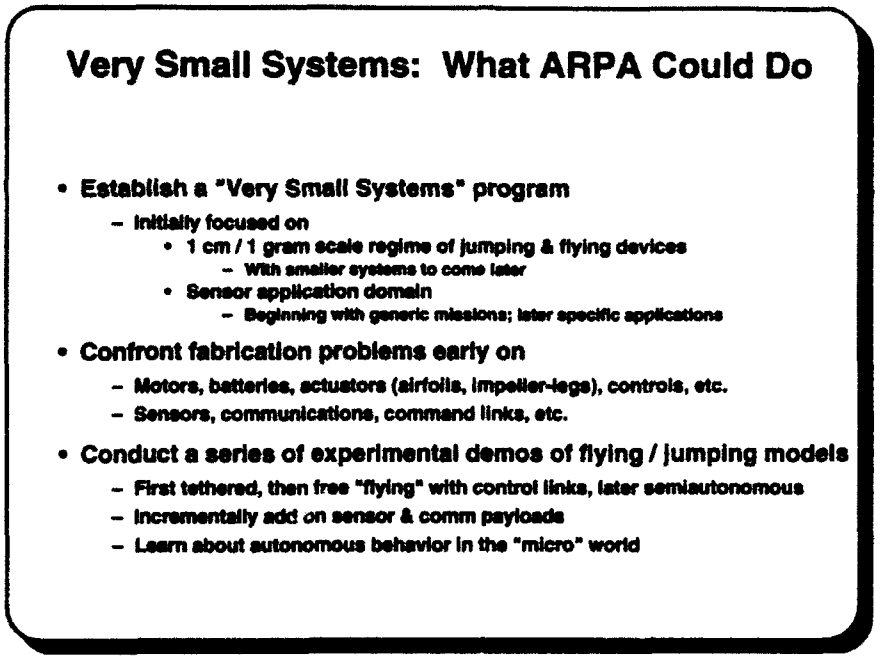
Stabilization and Navigation This will be one of the major challenges of any micro-vehicle design and test program. Typical issues include

---

[26]As one of many examples of the actuator design issues requiring attention: in a mini-helicopter, should one go to the trouble of having flap joints in the rotor?

how small miniature inertial guidance and automatic stabilization subsystems can be made, etc. As an incremental approach, initial steps could start off with tethered vehicles (for flying systems), or with external stabilization (for jumping systems), with a later transition to the more challenging, completely autonomous stabilization and navigation. Consideration could also be given to design possibilities that minimize orientation requirements (e.g., payloads that work regardless of orientation, etc.).

Control and Communications There are a number of miniaturization challenges here. The control and communications approaches currently used in clandestine "bugs" could serve as a useful point of departure.



Based on the perspective obtained during the workshop, a reasonable next step would be for ARPA to establish a "very small systems" program. Such a program should initially focus on the one centimeter, one gram scale regime of jumping and flying devices, with smaller systems to come later. The overall mission emphasis should be on the broad sensor application domain. Initially the program should deal in terms of generic missions, with a focus on specific applications delayed until later.

This should be a "doing" program, not just a study program. The program should be structured to confront fabrication problems early on, by building real micro motors, batteries, actuators, controls, sensors, communications systems, command links, etc.

A central part of the program should be the conduct of a series of experimental demonstrations of flying or jumping models. These demonstrations could first be tethered, then later free flying (or jumping) with control links, then still later semiautonomous.

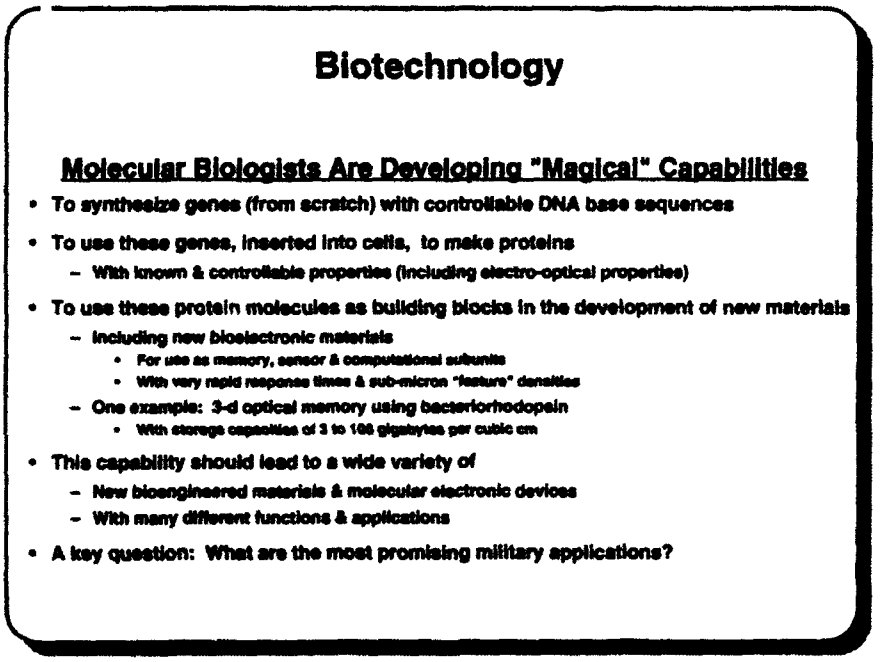
One of the primary objectives of this sequential series of experiments would be to learn about autonomous behavior in the "micro" world.[27]

---

[27]Just as the Carnegie Mellon NAVLAB II autonomous driving system had to learn what to do when it encountered other vehicles on a freeway, or obstacles when moving cross country, the micro-vehicles will have to learn how to deal with obstacles in the micro world.

3. Biomolecular Electronics

We now turn to a discussion of the second candidate ARPA program area: biomolecular electronics. This promising new technology area is an outgrowth of ongoing advances in the broader area of biotechnology. We begin with a capsule review of the most exciting—the most "magical"—of those advances, which are occurring in molecular biology.



Molecular biologists are developing a vast array of new capabilities. Among the most "magical" of these new and still evolving capabilities are:

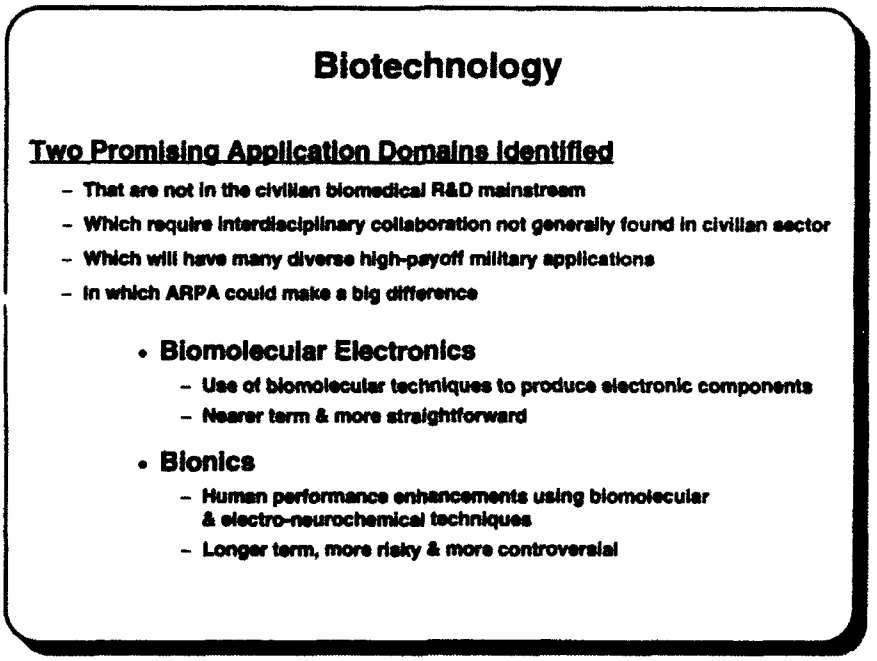
- The ability to synthesize genes from scratch, with controllable DNA base sequences.
- The ability to use these synthetic genes, inserted into cells, to make proteins with known and controllable properties.
- The ability to use these synthetic protein molecules in the development of new materials.

Electro-optical properties are among the protein properties that can be controlled and modified in this way. This process, when applied to electro-optical properties, can in principle lead to new bioelectronic materials, for potential use as memory, sensor, or computational subunits in future information processing systems.[28]

This capability should lead to a wide variety of new bioengineered materials and molecular electronic devices, with many different functions and applications. A key question, addressed during the ARPA workshop, is: What are the most promising military applications of this capability?

---

[28]Sligar and Salemme (1992) survey the use of bioengineered proteins as building blocks in molecular electronics and sensor materials applications. At least one such new bioelectronic material has already been developed, a three-dimensional optical memory based on the protein bacteriorhodopsin. This is discussed in Birge (1992) and in Birge and Gross (1992).



The discussions during the ARPA workshop identified two promising (military) application domains of biotechnology:[29]

- *Biomolecular electronics,* the use of biomolecular techniques to produce electronic components.
- *Bionics,* the use of biomolecular and electro-neurochemical techniques to produce human performance enhancements.

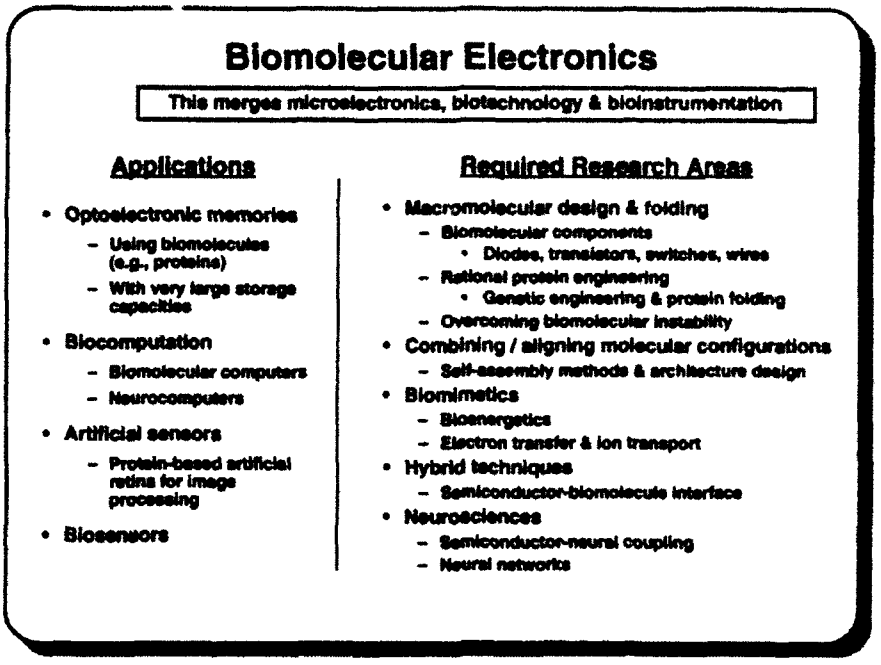
Neither of these areas is currently in the civilian biomedical research and development mainstream. Each of them will require a degree of interdisciplinary collaboration not generally found in the civilian sector. Each of them should have (ultimately) many diverse high-payoff military applications. And in each of these areas, ARPA could make a big difference.

Of these two areas, biomolecular electronics appears to be nearer term and more straightforward. Bionics is longer term, more risky, and (almost undoubtedly) more controversial.

We now discuss each of these areas in turn.

---

[29] At the request of ARPA, the workshop specifically excluded consideration of *medical* applications of biotechnology.



Biomolecular electronics merges the techniques of biotechnology and bioinstrumentation with those of microelectronics. Among its possible applications are:

- Optoelectronic memories, with various large storage capacities, using biomolecules.[30]
- Biocomputation, the use of biomolecules as computational building blocks, as well as the use of biological computational architectures.[31]
- Artificial sensors, such as protein-based artificial retinas for image processing.[32]
- Biosensors, for use in (among other things) detecting baterial-warfare (BW) agents.

Making a reality of these applications requires advances in a number of research areas, including:

- Macromolecular design and folding. One of the key issues here is protein folding: understanding and predicting the three-

---

[30]See Birge (1992a) and Birge and Gross (1992).

[31]Conrad (1992a), Conrad (1992b), Capstick et al. (1992), Hameroff et al. (1992), Aoki et al. (1992), Rambidi (1992), Birge (1992a), and Birge and Gross (1992) discuss various aspects of biocomputation.

[32]Chen and Birge (1992) discuss protein-based artificial retinas.

dimensional structures of proteins from their sequences of amino acids.[33]

- Combining and aligning molecular configurations, including self-assembly methods and architecture design.
- Biomimetics, including a better understanding of bioenergetics, electron transfer, and ion transport.
- Hybrid techniques, coupling microelectronics and biotechnology. One of the most important research issues here is the semiconductor-biomolecule interface, which will be present somewhere in all biomolecular electronic systems.
- Neurosciences, including not only neural networks, but also the semiconductor-neural coupling.

"Foundation" research in all of these areas will be required in any broad-based biomolecular electronics program.

---

[33]Chan and Dill (1993) review the current state of understanding of protein folding.

Why Biomolecular Electronics?
How Does It Compare? (1 of 2)

• Feature Size		
– Protein-based components	10^{-7} to 10^{-8}	meters
– Silicon-based IC elements	$\geq 2 \times 10^{-7}$	meters
• Switching Energies		
– Elemental biomolecular transitions	10 - 100 *KT*	10^{-19} joules
– Conventional electronics (per bit processed)	$\geq 10^{5}$ *KT*	10^{-15} joules
• Response Times		
– Opto-electronic transitions	10^{-12}	sec
– Intramolecular electron transfer	10^{-9} to 10^{-12}	sec
– Molecular shape changes	10^{-9}	sec
– Intermolecular ion transfer	10^{-3} to 10^{-4}	sec
– Enzyme lock-key pattern processing	10^{-3} to 10^{-4}	sec

During the workshop, we took a very preliminary look at how biomolecular electronic devices might compare with conventional microelectronic devices.

Regarding *feature size,* silicon-based integrated circuit elements fabricated using optical lithography are (probably) limited to scales of 0.2 microns or greater. Protein-based components should range in size (depending upon the size of the proteins involved) from 0.1 to 0.01 microns. This reduced feature size of biomolecular components should make possible greater memory and computational element densities.

Regarding *switching energies,* each elemental biomolecular transition typically consumes from 10 KT to 100 KT of energy, or about 10^{-19} joules.[34] This compares with at least 10^5 KT per bit processed for conventional microelectronics, or about 10^{-15} joules, some four orders of magnitude larger. These reduced switching energies offer the prospect of computers with vastly reduced power consumptions.[35]

Insofar as *response times* are concerned, biomolecular transitions cover a wide range. The fastest are opto-electronic transitions, such as those

---

[34] K = 1.381 x 10^{-23} joules/deg K is Boltzmann's constant, and T is the operating temperature of the device in degrees Kelvin.

[35] As one "existence-proof" example of what might be possible, the human brain performs 10^{12} to 10^{15} elemental operations per second, and consumes about one to 10 watts of power.

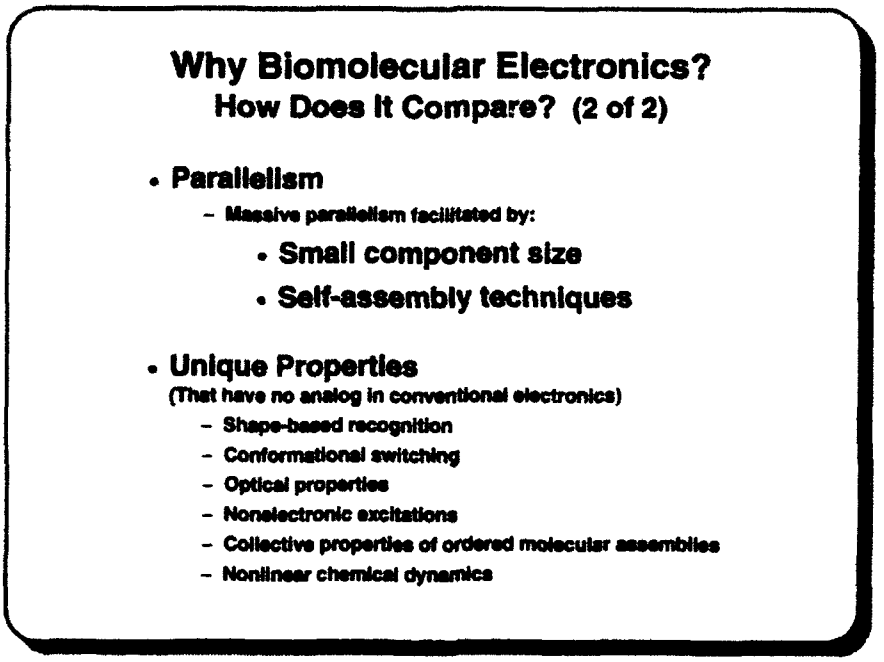
involved in the bacteriorhodopsin-based optical memory cited earlier.[36] These take about 10^{-12} sec. Transitions involving intramolecular electron transfer are somewhat slower, requiring 10^{-9} to 10^{-12} sec. Transitions involving molecular shape changes typically take about 10^{-9} sec. All three of these—opto-electronic transitions, intramolecular electron transfers, and molecular shape changes—are in principle fast enough to support gigahertz computational processing rates.

Some biomolecular transitions are much slower, however. For example, transitions involving intermolecular ion transfer or enzyme "lock-key" pattern processing take 10^{-3} to 10^{-4} sec. Biomolecular computers dependent on transitions of these types would have much slower serial processing rates.[37] However, the massive parallelism in principle possible with biomolecular-based computers could still result in very large overall processing rates. We discuss this on the next page.

---

[36]See Birge (1992).

[37]Some of the biomolecular transitions requiring the smallest switching energies may be associated with these slower response times.



The use of biomolecular components and biological assembly techniques should be conducive to massive parallelism, for (at least) two reasons:

- The small feature size possible with biomolecular components should lend itself naturally to massive parallelism.
- Biological, self-assembly techniques should be directly applicable to the fabrication of massively parallel computational architectures.

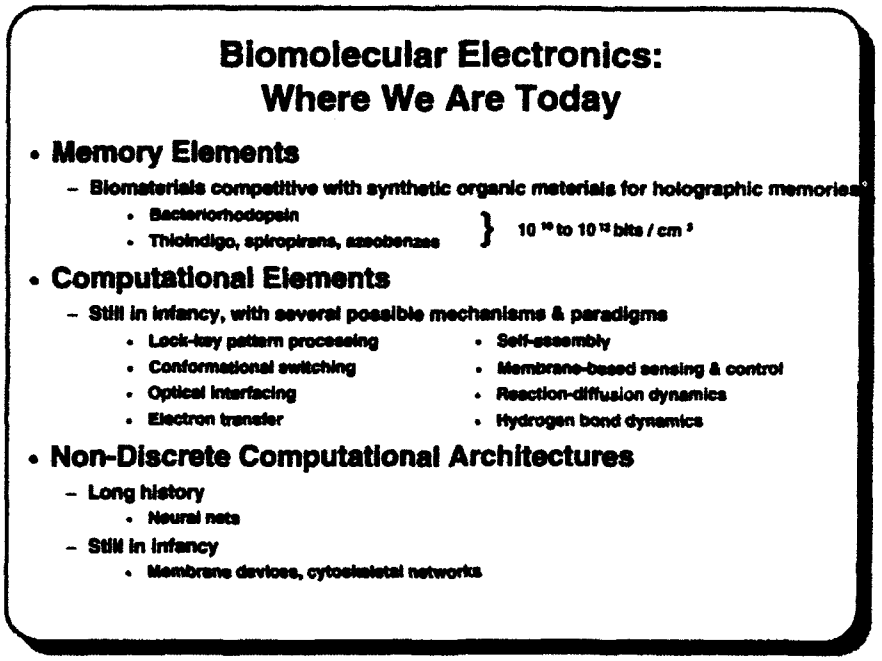
In addition to the substitution of biomolecular components for microelectronic components in conventional computer architectures, biological "computers"—i.e., the "things" performing computational functions in biological systems—have a number of unique properties that have no analog in conventional electronics. These include:

- Shape-based recognition, such as that used by enzymes in "lock-key" pattern processing.
- Conformational switching, in which the transition of a single electron into or out of a covalent bond changes the shape of a molecule.
- Optical properties, which can be highly specific to individual molecular states.
- Nonelectronic excitations. One example of these are the so-called "protein quakes," in which a molecule binds to a protein, thereby

stressing the binding site. When the molecule is released from the protein, this stress must be relieved, thereby propagating a stress wave through the protein.

- Collective properties of ordered molecular assemblies, which can lead to new, nondiscrete computational architectures.
- Nonlinear chemical dynamics.

These unique properties of biomolecules can lead to new types of computational devices.



Where is biomolecular electronics today? How much progress has been made toward achieving this promise?

With regard to *memory elements*, significant progress has already been made. Biomaterials such as bacteriorhodopsin have been developed with storage densities of 10^{10} to 10^{12} bits/cm^3.[38] These are competitive with the best synthetic organic materials (e.g., thioindigo, spiropirans, azeobenzes) for holographic memories.

Biomolecular *computational elements*, however, are still in their infancy. Several possible mechanisms and paradigms have been identified, including lock-key pattern processing, conformational switching, optical interfacing, electron transfer, self-assembly, membrane-based sensing and control, reaction-diffusion dynamics, and hydrogen bond dynamics, but most of the important details remain to be worked out.[39]

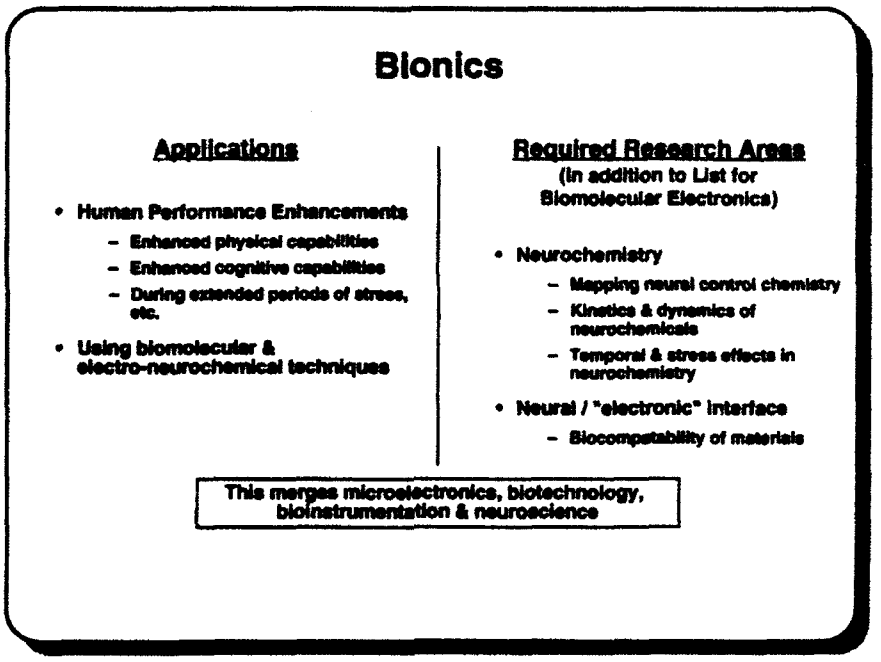
Insofar as *non-discrete computational architectures* are concerned, there is a long history of research on neural nets. Other non-discrete architectures, such as membrane devices or cytoskeletal networks, are still very much in their infancy.[40]

---

[38]Birge (1992) and Birge and Gross (1992) provide a detailed discussion of the development of bacteriorhodopsin-based optical memories.

[39]Conrad (1992b), Capstick et al. (1992), and Aoki et al. (1992) discuss a variety of biomolecular computational elements.

[40]Rambidi (1992) and Hameroff et al. (1992) provide examples of possible non-discrete biomolecular computing.



We turn now (briefly) to bionics: the use of biomolecular and electro-neurochemical techniques to produce human performance enhancements. Some of the possible performance enhancements that have been discussed by researchers are:[41]

- Enhanced cognitive capabilities, such as:
  - Improved vigilance and attention span,
  - Improved stress tolerance,
  - Reduced fatigue, drowsiness, and need for sleep,
  - Improved learning and memory.
- Enhanced physical capabilities, such as:
  - Exoskeletons for load-bearing and strength enhancement,
  - High-resolution night-vision bio-devices.

These applications are much further out than those discussed previously for biomolecular electronics. Making a reality of them requires advances in all of the research areas listed previously for biomolecular electronics, as well as additional advances in:

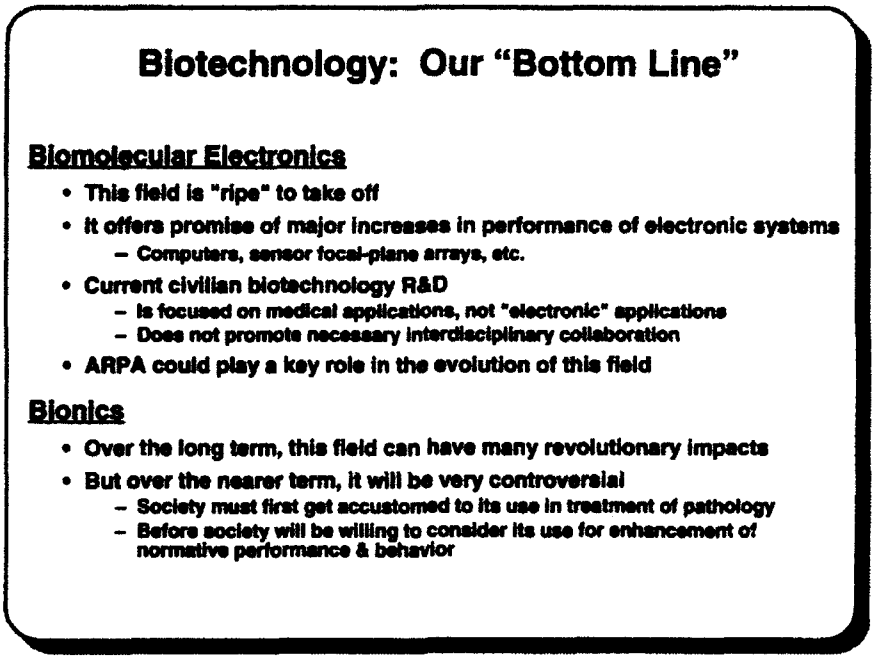
---

[41]The "Bionic Man" of TV history is not a bad picture of what some people are thinking of here.

- Neurochemistry, including the mapping of the neural control chemistry, the kinetics and dynamics of neurochemicals, and temporal and stress effects in neurochemistry.
- The neural-electronic interface, and the biocompatibility of "electronic" materials.

Much of this neurochemical research will be carried out by the medical research profession in the normal course of events, as they develop new techniques to treat various pathologies.

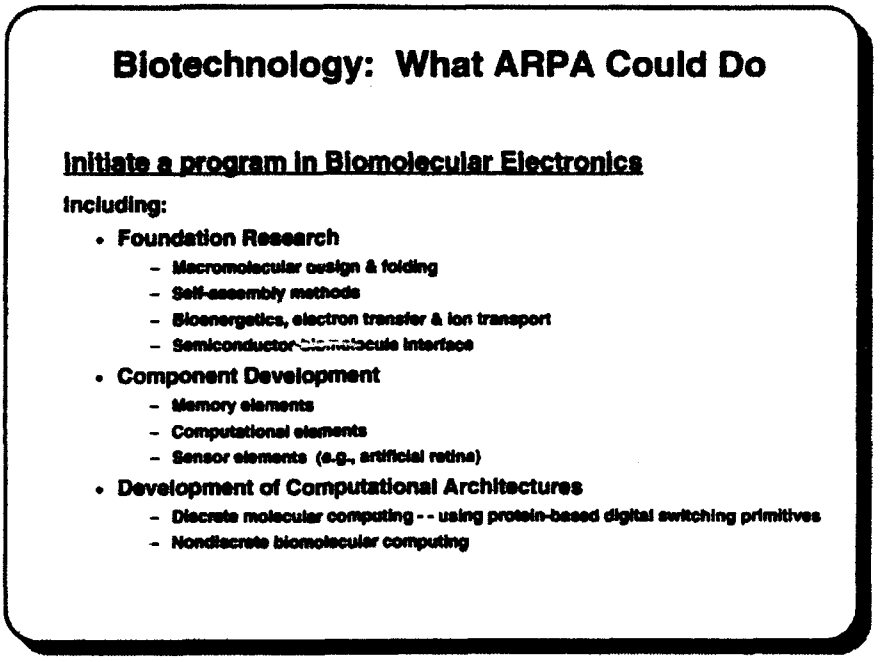
This is undoubtedly a high-payoff research area. It is also a high-risk area, and what may be more important, it is likely to be very controversial, since many people will look upon it as "interfering with the human brain."



Based on these considerations, the workshop reached the following conclusions concerning biotechnology:

- Ultimately, biotechnology should have major impacts in many areas of society in addition to health care, the area which has been the original motivation for much of the research. Two of the likely areas are biomolecular electronics and bionics.
- *Biomolecular electronics* is a field which is "ripe" to take off. It offers the promise of providing major increases in the performance of a wide variety of electronic systems: computers, sensor focal-plane arrays, etc. Current civilian biotechnology research and development activities are focused almost entirely on medical applications, with very little effort on "electronic" applications. In addition, these current R&D activities do not promote the interdisciplinary collaboration necessary for advances in biomolecular electronics. ARPA could play a key role in the evolution of this field.
- Over the long term, *bionics* should have many revolutionary impacts. However, it is not as ready to take off as biomolecular electronics. Even more important, over the near term this field should be very controversial. Society will have to get accustomed to the application of biomolecular and electro-neurochemical techniques in the treatment of pathology before it will be willing to consider their use for the enhancement of normative performance and behavior.

So for the time being, we believe that ARPA should focus on biomolecular electronics.



What could ARPA do? ARPA could initiate a program in biomolecular electronics. This program should have three components:

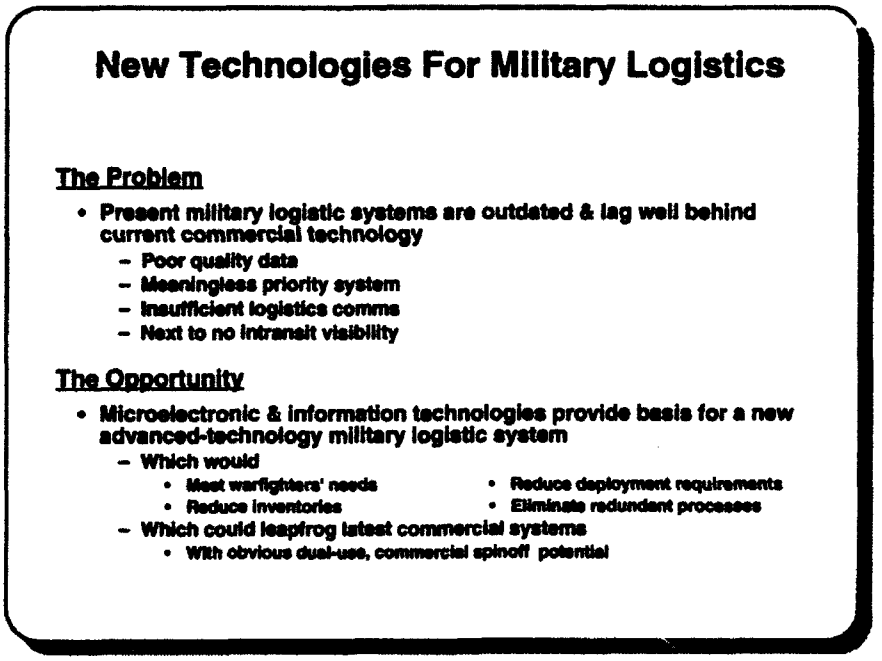
Foundation Research A series of research projects in macromolecular design and folding; self-assembly methods; bioenergetics, with a focus on electron transfer and ion transport; and the semiconductor-biomolecule interface. This activity would use the existing body of research in molecular biology as a point of departure and establish the broader foundations needed for applications in biomolecular electronics.

Component Development A number of research projects developing biomolecular-based components for use in current computational and sensor architectures, as substitutes for "electronic" components. Such biomolecular components would include memory and computational elements, and sensor elements, such as the artificial retina.

Development of Computational Architectures Research on new computational architectures, using biologic systems as examples. This could include discrete molecular computing using protein-based switching primitives, and nondiscrete biomolecular computing.

4. New Technologies for Military Logistics

We now turn to the third candidate ARPA program area: new technologies for military logistics.



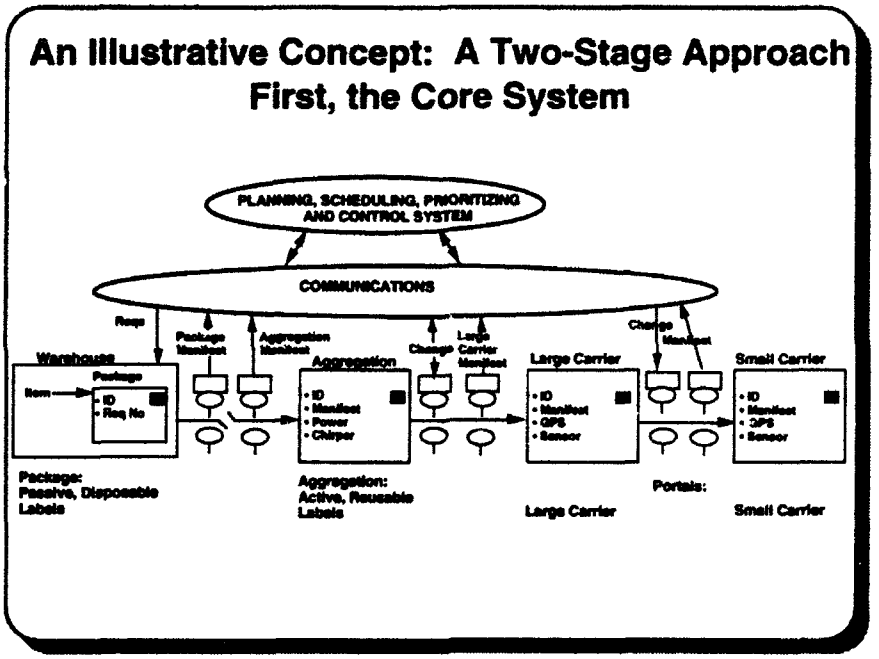
The *problem* here is well known: present military logistic systems are outdated and lag well behind current commercial technology. Today's military logistic systems must make do with (relatively) poor quality data on the status of the items in their inventories, make use of priority systems that have become increasingly meaningless in practice,[42] often must make do with insufficient communications, and frequently have little or no in-transit visibility on the status of shipments.

That is the problem. Modern microelectronic and information technologies provide an *opportunity*—for a new advanced-technology military logistic system that would solve this problem and would meet warfighters' needs, reduce the requirements for inventories, reduce deployment requirements (for tonnage of lift), and eliminate redundant processes.

At the same time, these new advanced-technology logistic systems could leapfrog the latest commercial systems. This would have obvious dual-use, commercial spinoff potentials.

---

[42]The deliberate escalation of priorities to obtain a place in the logistic queue and duplication of supply requests to increase the probability of receiving resupply have unfortunately become common practices.



There are many ways in which such an advanced-technology logistic system could be realized. We sketch out one concept here, merely as an illustration of a much broader class of system realizations.

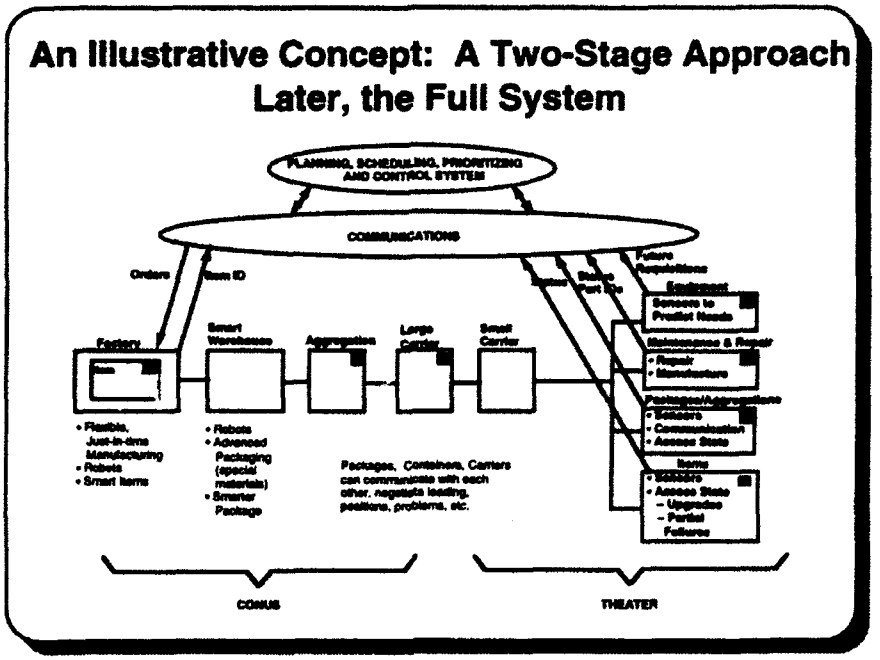
The concept described here involves a two-stage approach: a *Core System* and the *Full System.* This chart shows the Core System. Its three key components are:

- Smart chips
  - Every object in the logistic system has a smart chip embedded in it. This includes the supply item itself, the package it goes into, the larger container (termed an "aggregation" in the chart), and the carriers (both large and small) that transport the containers. These smart chips carry information on:
    - The catalog number, serial number, size, quantity, etc. of the supply item.
    - The manifest of the package.
    - The manifest of the containers and carriers, their location (provided by miniature GPS receivers), and their intended destination.
- Portals
  - Every time an object (supply item, package, container, etc.) changes its state, it goes through an electronic "portal," which

reads and updates the information contained on the object's smart chip and generates a *change message*. When a supply item is put into (or taken out of) a package, it goes through an electronic portal, which reads the smart chip contained in the item, updates both the chip in the item (to identify which package it is now in) and the chip on the package (to add the item in question to the manifest of the package), and generates a change message. Similar processes occur when a package is put into (or taken out of) a container, and when a container is put into (or taken out of) a carrier.

- Communications
  - A worldwide communications system transmits all of the change messages to a logistic control system. One convenient way to implement such a communications system would be by means of a Global Grid. In this realization, each individual portal would only have to transmit its change messages to the nearest Global Grid entry point, with the Global Grid backbone responsible for getting the messages the rest of the way to the nearest node of the logistic control system.
- Planning, scheduling, prioritizing, and control system
  - A worldwide distributed control system maintains up-to-date status information on all of the objects in the logistic system: individual supply items, packages, containers, and carriers.

In the Core System, the smart chips and portals are used to maintain status information and control all of the way "upstream" in the logistic system to the items in the warehouse and all of the way "downstream" to the supply depots nearest the point of use in the field.

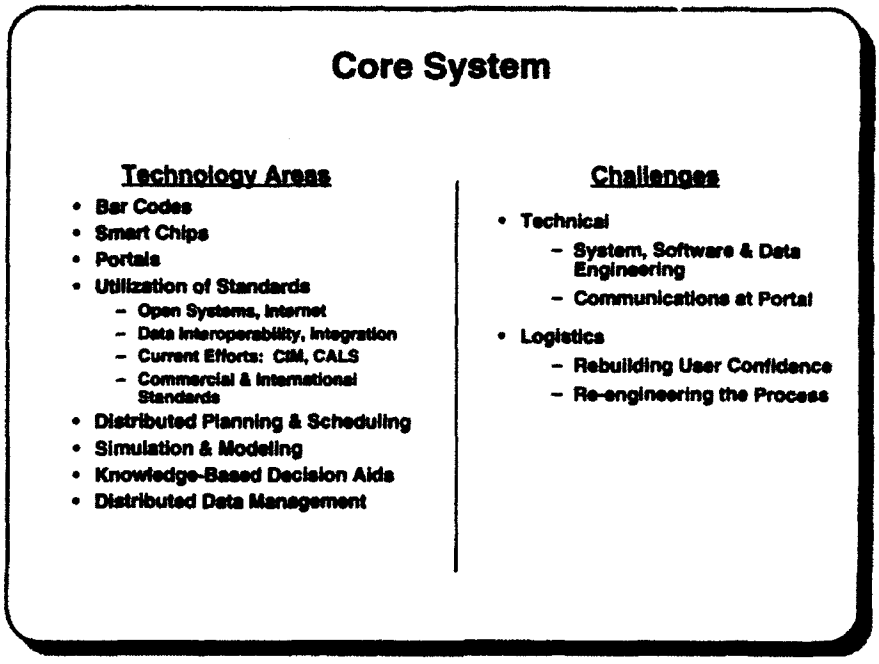


In the Full System, this concept of smart chips, portals, communications, and an overall logistic control system is extended even further upstream in the logistic system to the production line in the factory where the supply item is fabricated, and even further downstream to the equipment in use in the field and the maintenance and repair facilities supporting that equipment.

Sensors and smart chips on the operational equipment measure consumption and "wear," and predict future logistic needs—for example, measuring bearing wear to predict when replacement bearings will be needed—which they report via the communications system to the logistic control system. Smart chips in the maintenance and repair facilities report on the status of parts that have suffered total or partial failures, have been replaced or repaired in the field, etc.

All of this information, plus the in-transit status information supplied by the smart chips and portals associated with the warehouses, packages, containers, and carriers, is used by the logistic system control system to provide just-in-time manufacturing orders to the factory production lines.

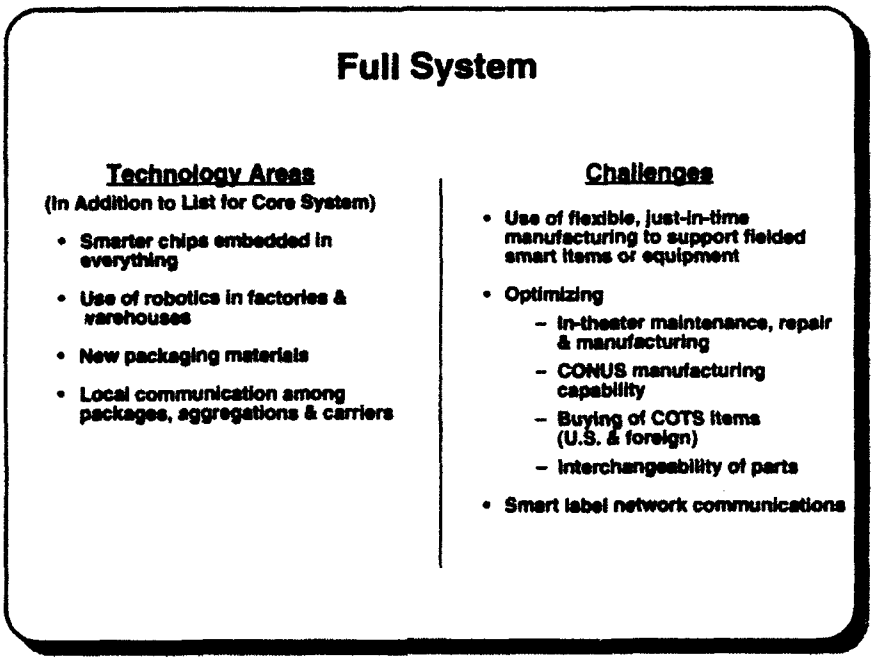
This Full System concept envisages a logistic system that is "wired together" in a "smart" way, all the way from the production lines in the factories to the in-use equipment in the field.



This chart lists the technologies that are required to establish the Core System. Most of these are available today (e.g., bar codes and smart chips). The electronic portals will have to be developed, but this should be straightforward, utilizing current sensor and microelectronic state-of-the-art. Likewise, development of the required standards, distributed planning and scheduling algorithms, simulation and modeling capabilities, knowledge-based decision aids, and distributed data management is well within current state-of-the-art.

The true challenges in the Core System are:

- Technical
  - The system, software, and data engineering of the overall system.
  - The design and implementation of the communications at the portals.
- Logistics
  - Rebuilding user confidence in the new system, so users will believe in it and use it properly.
  - "Re-engineering" the entire military logistic process.



The Full System requires all of the technologies involved in the Core System, plus:

- Even smarter ships embedded in everything, from the factory production line to the equipment operating in the field.
- The use of robotics in factories and warehouses.
- New packaging materials.
- Local communication among packages, aggregations, and carriers.

The biggest challenges in making the Full System a reality are:

- The use of flexible, just-in-time manufacturing to support fielded smart items and equipment.
- Optimizing a large number of interrelated activities, including in-theater maintenance, repair, and manufacturing; CONUS manufacturing; the buying of U.S. and foreign COTS (commercial-off-the-shelf) items; and the interchangeability of parts. (In order to realize the true performance potential of the Full System, the role that each of these activities plays needs to be optimized across the overall logistic system, rather than being sub-optimized within separate subsections of the overall system.)
- Smart label network communications.

What could ARPA do in this area? ARPA could establish a logistic focus somewhere within the agency. The new program associated with this logistic focus should concentrate on dual-use technologies. Some of the highest leverage ones on which to concentrate are:

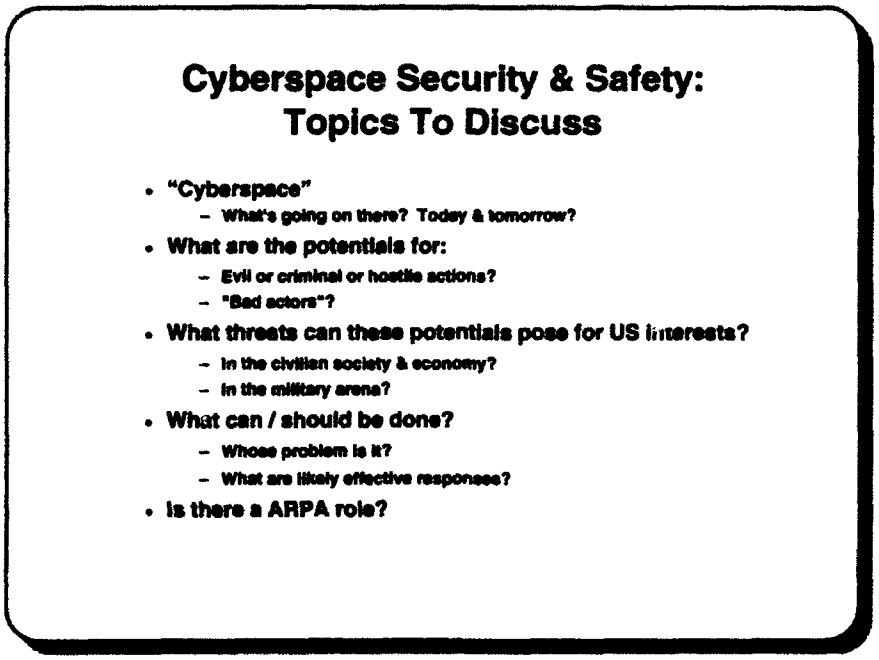
- Multi-function smart labels
  - Used throughout both the Core and Full Systems.
- Smart packaging material
- Package-to-portal communications
  - An essential element of both the Core and Full Systems.
- Distributing computing for planning, scheduling and prioritizing
  - Another essential element of both systems.

This new program should aim for early joint demonstrations:

- Joint in the ARPA/service sense of involving selected materiel support organizations from one or more of the military services.
- Joint in the military/civilian sense of involving a few civilian firms.

5. Cyberspace Security & Safety

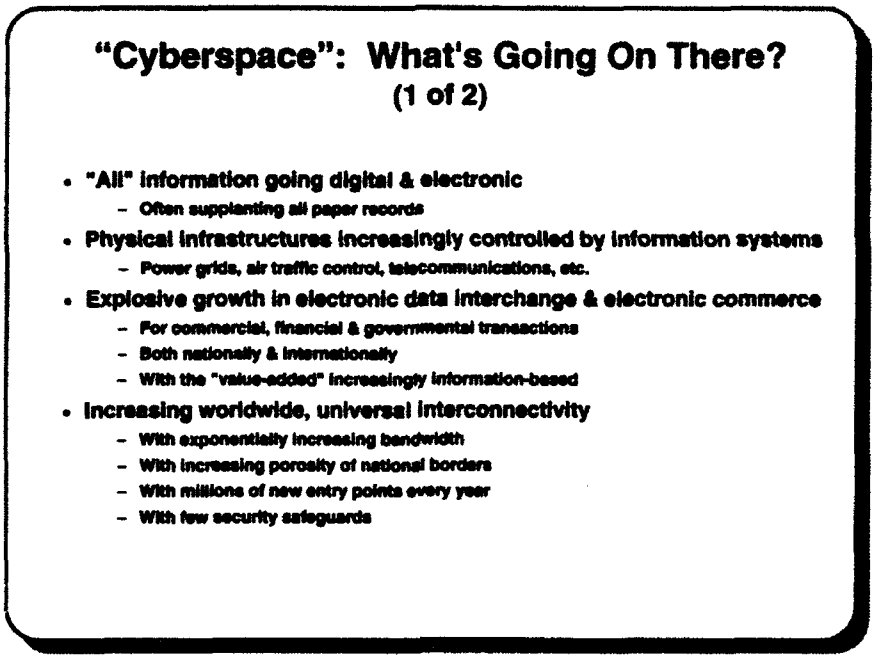
The fourth candidate ARPA program area is cyberspace security and safety: the development of techniques and strategies to protect U.S. interests in and relating to "cyberspace"—the global world of internetted computers and communication systems in which more and more U.S. activities (military and civilian, governmental and non-governmental, economic and social) are being carried out.



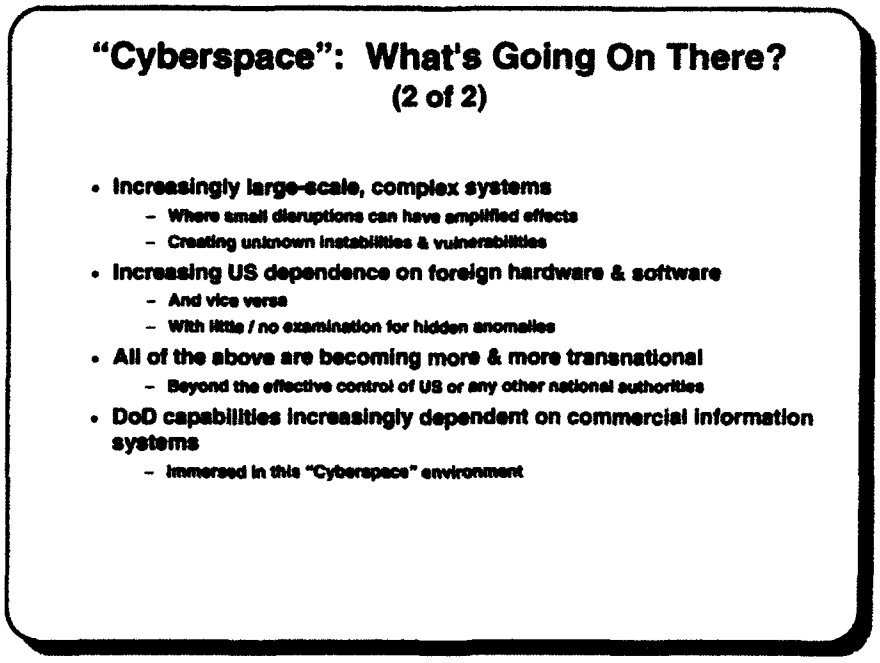
We begin with a short discussion of cyberspace: what it is, what is going on there, and why it is important. Next, we outline the emerging potentials for:

- Evil, criminal or hostile actions in cyberspace.
- "Bad actors" in cyberspace, carrying out these "evil" actions.
- Threats to U.S. interests, as a result of the bad actors carrying out hostile actions in cyberspace.

Following that, we discuss what needs to be done to cope with this problem, and identify a role that ARPA could play.



As one consequence of the electronic digitization of information and the worldwide internetting of computer systems, more and more activities in the U.S. and throughout the world are mediated and controlled by information systems. This includes human activities of all kinds: research and educational activities, commercial business and financial transactions, engineering and industrial processes, operations of civil governments at all levels (national, regional, local), military operations, political activities, both public and private social interactions, and even the operation of essential physical infrastructures. The global world of internetted computers and communications systems in which more and more of these activities are being carried out has come to be called "cyberspace."

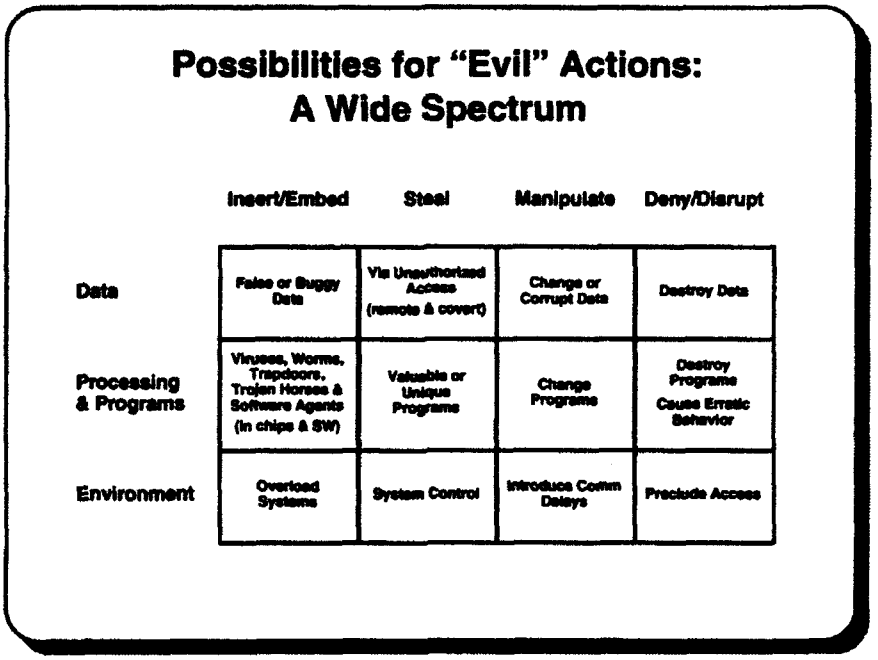


As time goes on, these internetted information systems operating in cyberspace form increasingly large-scale, complex systems, in which small disruptions can have amplified effects, creating unknown instabilities and vulnerabilities.

At the same time, the U.S. is becoming increasingly dependent on foreign information hardware and software. The same is also true for all other nations. Today there is little or no examination of this foreign hardware by anybody—in the U.S. or any other nation—for hidden anomalies.

All of these activities in cyberspace are becoming more and more transnational, beyond the effective control of the U.S. or any other national authorities.

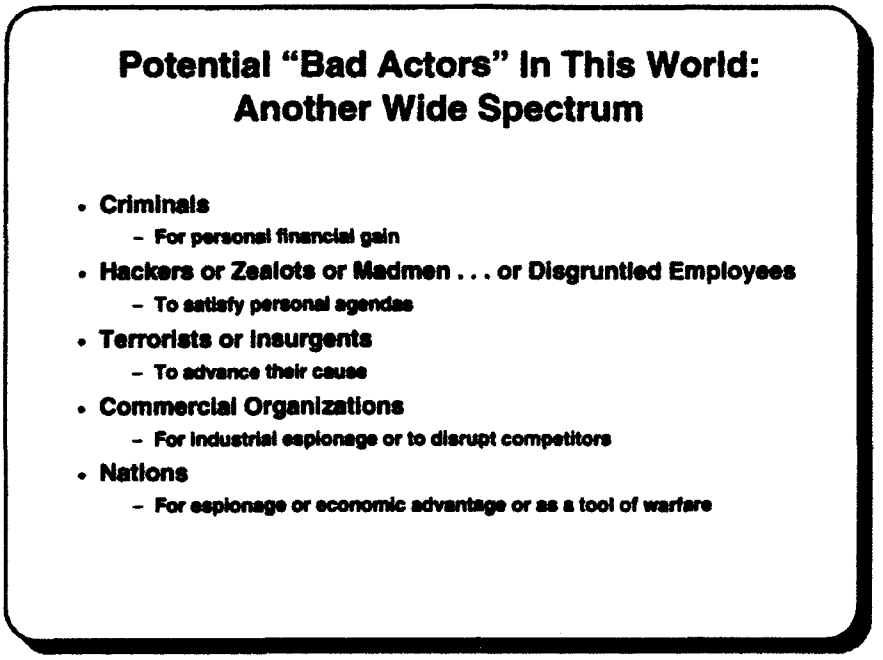
Finally, more and more DoD capabilities are becoming increasingly dependent on commercial information systems which are immersed in this cyberspace environment.



The information systems mediating and controlling these various activities in cyberspace are subject to a broad spectrum of "evil actions," as illustrated in this chart. These include attacks on the data contained within the systems, the programs and processing hardware running those systems, and the environment (communications, networks, etc.) in which they operate. The spectrum of possible evil actions includes:

- Inserting false data or harmful programs (viruses, worms, etc.) into information systems.
- Stealing valuable data or programs from a system, or even taking over control of the operation of a system.
- Manipulating the performance of a system, by changing data or programs, introducing communications delays, etc.
- Disrupting the performance of a system, by causing erratic behavior or destroying data or programs, or by denying access to the system.

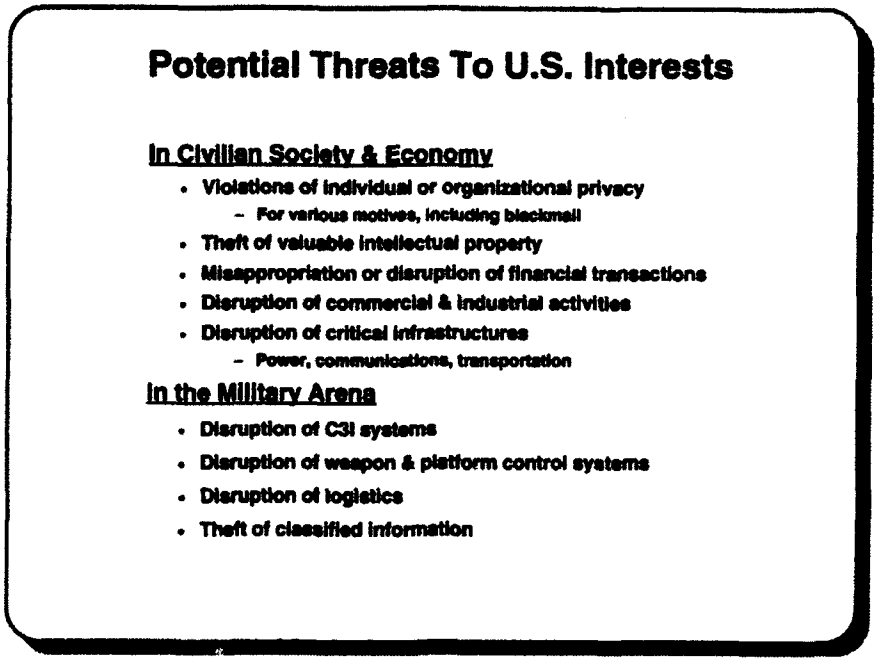
All of these evil actions can be done surreptitiously. Many of them can be done remotely, at a great distance from the target system—sometimes from the other side of the world—via a series of internetted, intermediary systems. Taken together, the surreptitious and remote nature of these actions can make their detection difficult and the identification of the perpetrator even more difficult.



This gives rise to a new set of vulnerabilities—for governments, the military, businesses, individuals, and society as a whole—that can be exploited by a wide spectrum of "bad actors" for a variety of motives, as indicated on this chart.

In this cyberspace world, the distinction between "crime" and "warfare" is blurred. The resources required for a nation to mount a computer-based attack on the military, economy, or society of another nation (presumably an act of war) are not necessarily any larger than those required for an individual to mount a criminal attack on another individual, company, bank, etc. In each case all that may be required is one (or at most a few) smart computer expert with a computer terminals hooked into the worldwide network.

This blurring of the distinction between "crime" and "warfare" in cyberspace also blurs the distinction between police responsibilities to protect U.S. interests from criminal acts in cyberspace, and military responsibilities to protect U.S. interests from acts of war in cyberspace.



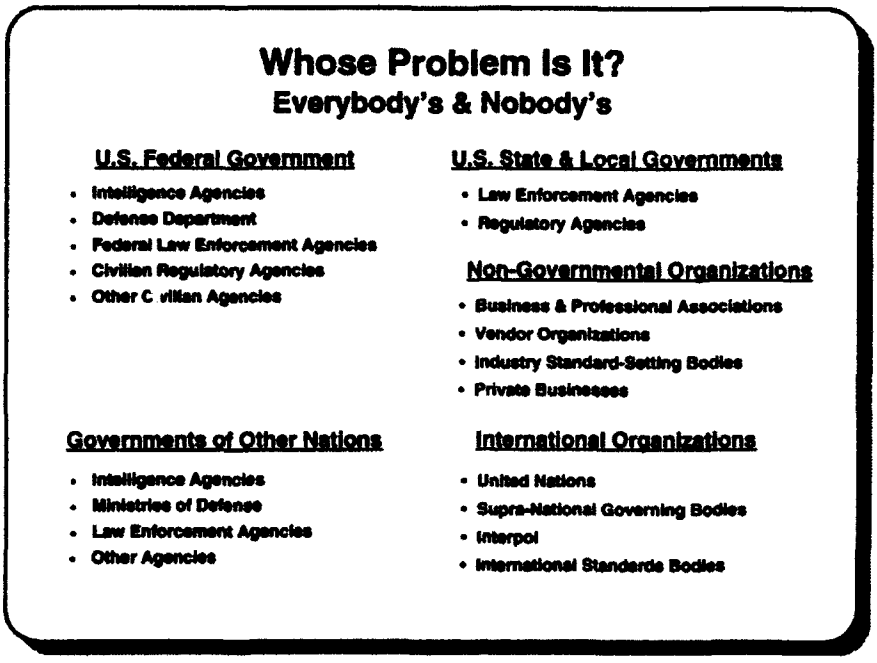
These possibilities for evil actions in cyberspace and this spectrum of potential bad actors lead to a new set of potential threats to U.S. interests, in both the civilian society and economy and in the military arena. This chart indicates some, but by no means all, of these new and emerging threats to U.S. interests. We have already seen examples of several of these actually occur.[43]

Protecting government, business, individuals, and society as a whole against these evil actions by bad actors in cyberspace we call "cyberspace security."

In addition to these deliberate threats, information systems operating in cyberspace, when embedded in their operational environments, can also cause unforeseen actions or events—without the intervention of any bad actors—that create unintended (potentially or actually) dangerous situations for themselves or for the physical and human environments in which they are embedded. Protection against this additional set of cyberspace hazards we call "cyberspace safety." In the new cyberspace world, government, business, individuals, and society as a whole require both "security" and "safety" protections: i.e., a comprehensive program of cyberspace security and safety (CSS).

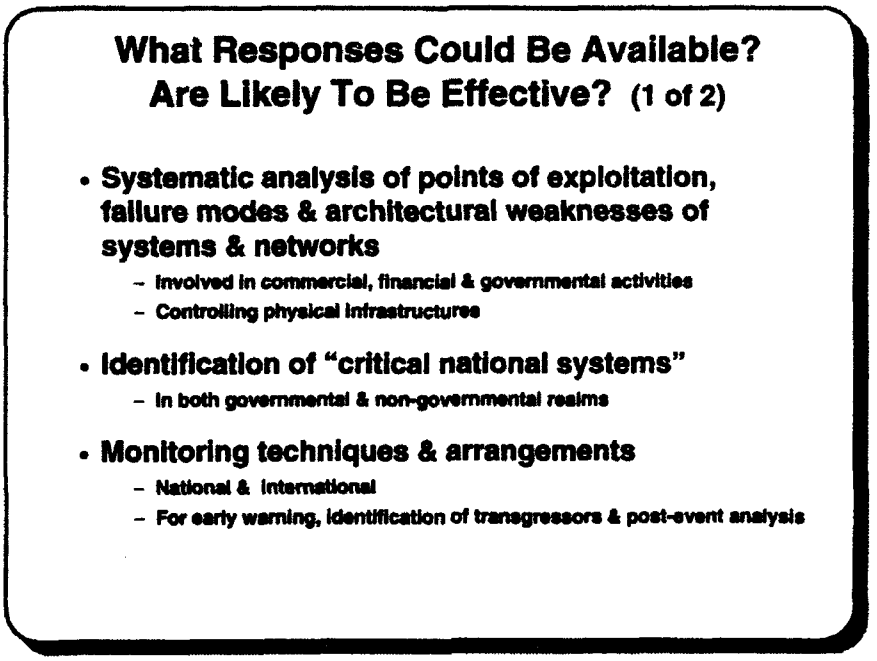
---

[43]Two (among many) notable examples were the "Internet Worm," which disrupted activities on the Internet in 1988, and the "Hannover Hacker," who stole information from computer files all over the world during 1986-1988 and sold it to the KGB. (The story of the Hannover Hacker is told in *The Cuckoo's Egg* by Clifford Stoll.)



Responding to this new, emerging security and safety "threat" and providing these CSS protections require activities coordinated across many organizational boundaries: military and civilian agencies of the U.S. government; federal, state and local agencies; both governmental and non-governmental entities; the U.S. and other nations; and national and international organizations. Today this is "everybody's" problem, and therefore "nobody's" problem. It falls into all of the "cracks."

ARPA can play an important role in beginning to fill these cracks by setting the initial direction for U.S. activities in CSS and serving as a catalyst to stimulate the interest and involvement of other agencies and organizations in the problem. This requires an ARPA program in CSS that identifies and develops technical safeguards and protective procedures, and also includes a set of "outreach" activities explicitly designed to spread awareness of the CSS problem and involve other organizations, both governmental and non-governmental, in the implementation of solutions.



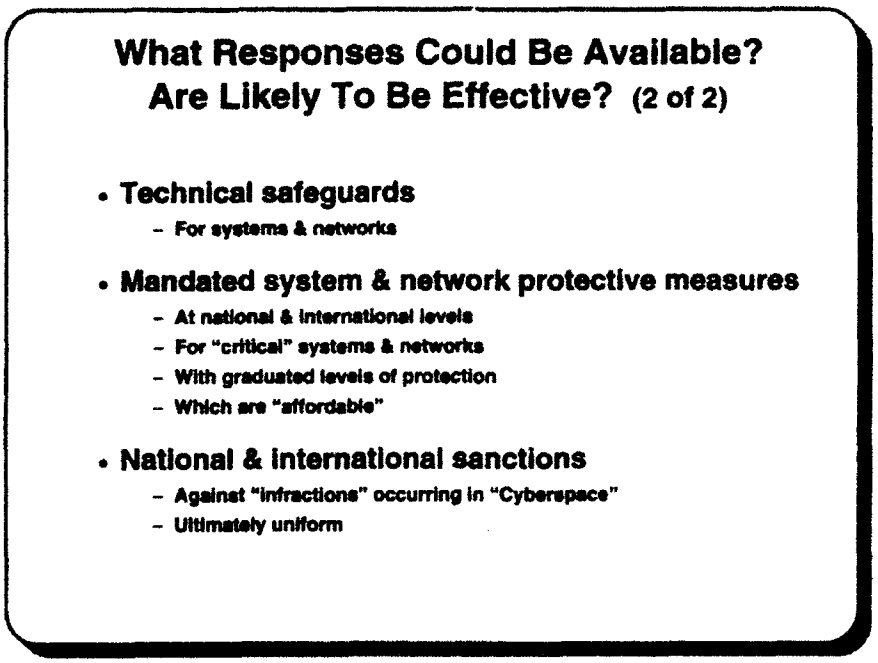
What responses could be available, as part of such a CSS program, and are likely to be effective?

Effective responses should include:

- The systematic analysis of points of exploitation, failure modes, architectural weaknesses, and safety hazards of U.S. information systems and networks, including those involved in commercial, financial and governmental activities, as well as those controlling physical infrastructures.
- The identification of "critical national systems and networks," in both the governmental and non-governmental realms, which should receive special attention in the program, and the development of prioritized vulnerability and hazard roadmaps for these systems and networks.[44]
- The development of monitoring techniques and arrangements, for early warning of threatening events in cyberspace, the identification of transgressors, and post-event analysis.

---

[44]A system or network may be deemed "critical" for many different reasons: because it provides essential support to vital physical or financial infrastructures; because its compromise could jeopardize the safety or well-being of large numbers of U.S. residents, or their financial security, or even merely their piece of mind; because its pervasive use for valued functions in society offers a widespread target for bad actors; because it plays a vital national security role; etc.



The development of technical safeguards is an obvious, integral component of any program of cyberspace security and safety. These safeguards should emphasize network security and safety, as well as computer security and safety, with particular emphasis on heterogeneous networks.

To be effective, the responses should also include:

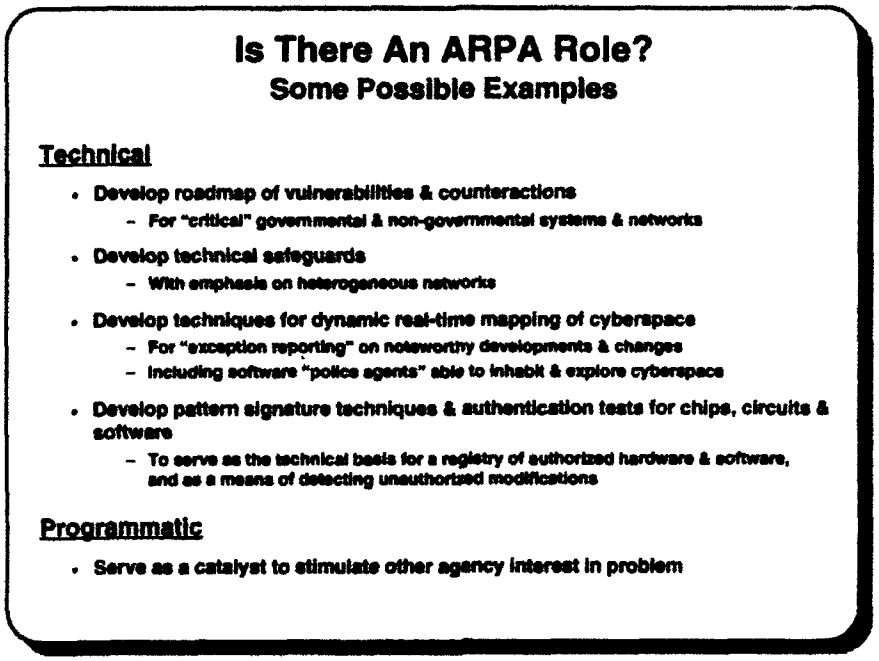
- Mandates (legal or otherwise) to compel or at least strongly urge people to use available protective measures on their information systems. The mandated measures must appear reasonable and "affordable" to their user community.
- Sanctions (legal or otherwise) against "infractions"—the perpetration of "evil actions" or the operation of unsafe systems—in cyberspace. Because of the transnational character of many/most activities in cyberspace, these sanctions may ultimately have to be international in scope to be truly effective.

What About "Offensive" Exploitations Of These New Vulnerabilities?

As An Intelligence Or Military Technique

- **What could the U.S. do?**
- **What should the U.S. do?**

A U.S. program in cyberspace security and safety is a defensive response to these new vulnerabilities. An offensive response is also possible. These vulnerabilities in cyberspace could be exploited by the U.S. for intelligence or military purposes. Discussion of this aspect of the problem is beyond the scope of this report.



As we mentioned earlier, ARPA could play an important role in setting the initial direction for U.S. activities in CSS and serving as a catalyst to stimulate the interest and involvement of other agencies and organizations in the problem.

This chart lists some specific technical activities that ARPA could undertake as major components of a program performing this catalytic role:

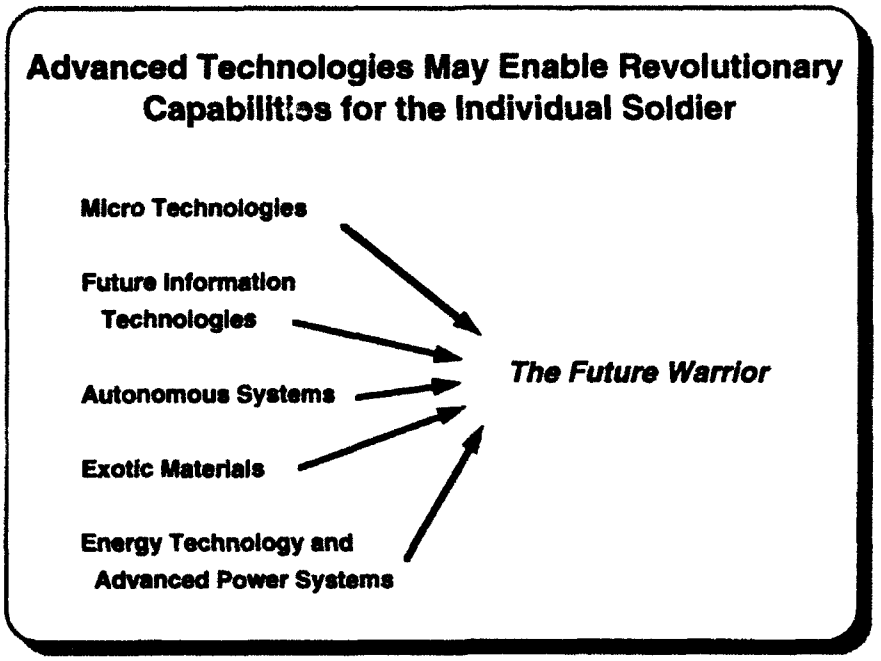
- The development of a roadmap of vulnerabilities, for critical governmental and non-governmental systems and networks.
- The development of technical safeguards, with an emphasis on heterogeneous networks.
- The development of techniques for dynamic real-time mapping of cyberspace, for exception reporting on noteworthy developments and changes.
- The development of pattern signature techniques and authentication tests for chips, circuits, and software, to serve as the technical basis for a registry of authorized hardware and software, and as a means of detecting unauthorized modifications.

6. Performance Enhancers for the Individual Soldier

The "Jedi Knight"

The final candidate ARPA program area is the "Jedi Knight," the name the workshop chose to denote performance enhancers for the individual soldier.

ARPA and the services have long-standing programs evolving the concept of a "Super Soldier," a combatant who (ideally) could be all-sensing, covert, indestructible , brilliant, and lethal. Recent technological advances have made it possible to begin realizing some of these functions for the future warrior. During the workshop we identified the most critical technological advances needed to enable this revolutionary concept.



The genesis of the Jedi Knight concept arose out of the exploration of technology areas in the first workshop session. Five key technology areas were seen as offering promise to greatly amplify the capabilities of today's individual soldier:

- Micro technologies could provide him with miniature sensors, monitors, and display systems.
- Future information technologies could link the soldier horizontally and vertically in the force, and even to distant sensors and databases.
- Autonomous systems such as unmanned ground vehicles (UGVs) and unmanned air vehicles (UAVs) could give him platforms for sensing, weapons, and mobility.
- Exotic materials could provide the soldier with protective clothing providing some degree of armoring and signature reduction.
- New energy technologies, finally, are needed to efficiently power the many components of this future warrior.

The Concept

- **Provide enhanced capability for a few specialized soldiers, acting individually or in a combat team, to achieve performance beyond normal levels**
- **Allow stealthy penetration (insertion & extraction) into a combat zone**
- **Facilitate local management of information & combat assets**
- **Provide long range surveillance & targeting information**

The Jedi Knight concept is that of an individual soldier who can be stealthy and lethal on his own while at the same time a member of a combat team connected into a global information and command network. The Jedi Knight is intended to be quickly inserted into a combat zone, assess the situation, carry out an orchestrated, surgical mission, and return with minimum losses.

Five Representative Missions Anticipated For The Jedi Knight

Mission	Duration
1) Airfield Seizure	Several hours
– Capture & secure perimeter	
2) Hostage Rescue	Several hours
– Infiltrate & retrieve hostages	
3) Long Range Reconnaissance & Patrol	Few days
– Deep battlefield surveillance & target designation	
4) Raid	Few days
– Penetrate & destroy key targets (e.g., command centers & early warning air defense)	
5) Urban Warfare	Days to weeks
– Reclaim & secure buildings & area	

The types of missions suited to the Jedi Knight concept are primarily small-scale contingency operations, missions falling into the "Type C" category of the 1992 OSD Net Assessment summer study. Such missions can range from those involving individual soldiers to coordinated attacks with naval, ground, and air support.

The Jedi Knight is envisioned to perform these missions either by using "onboard" weaponry or by providing targeting information for remotely managed weapons. These missions can last from hours to weeks, resulting in special needs for endurance and resupply.

Key System Factors

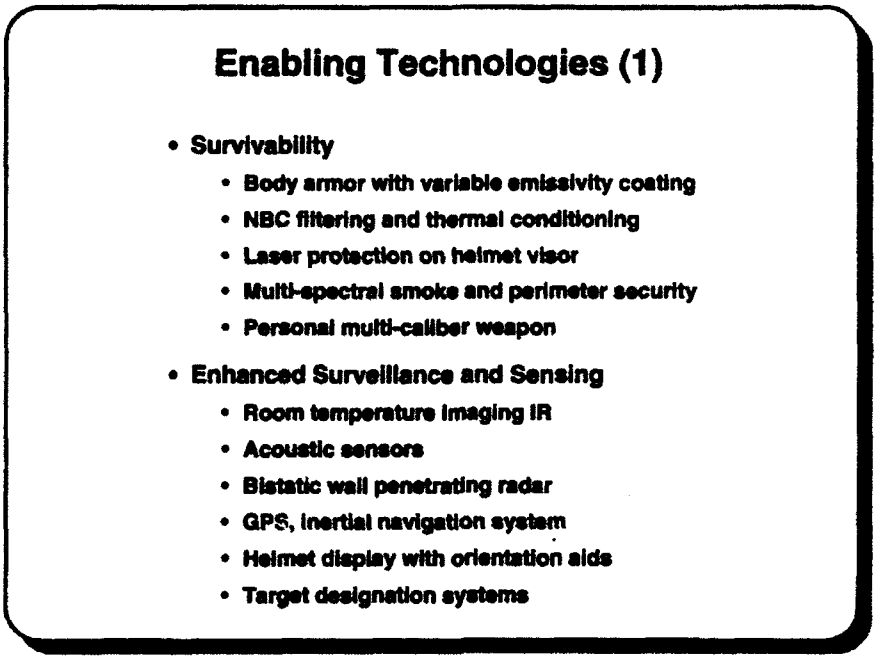
- **Survivability**
- **Enhanced surveillance & sensing**
- **Command, control, communications & robust computation**
- **Physiological monitoring & medical aids**
- **Stealthy deployment & extraction**

All in a self-contained package with compact power supply, with ability to operate individually or as a member of a squad

In considering these conceptual missions, we found that five areas stand out as desired system characteristics or requirements:

- The Jedi Knight has to be survivable, through armor protection, stealth, surprise, and quickness.
- He has to be able to sense, recognize and locate threats accurately at long range. He must also be able to report his findings, respond on his own with personal weapons, or call in fires.
- He has to be an integral part of a global C4I network, able to covertly query information, assess the situation, relay data, and accept commands.
- For safety and efficiency, he needs physiological monitoring and automated medical aids.
- Finally, Jedi Knight needs deployment mobility—some means of getting into and out of the area of operation using stealth for survivability.

Once on the ground, we do not envision mechanical exoskeletal aids for added strength or speed because of the associated weight, bulk, and power requirements. The Jedi Knight needs light, compact equipment that will not burden cross-country mobility.



Survivability technologies are paramount in the Jedi Knight concept. It should be possible to provide a lightweight, next generation kevlar-like bodysuit able to stop small arms fire, artillery fragments, and flame, using technologies available today or under development.[45] This suit could provide reduced observables, matching the background with a variable emissivity skin using electrochromics or other technology.[46] The bodysuit could also have NBC sealing and some form of thermal conditioning, although power supplies for more than short periods may be too heavy for the soldier. The Jedi Knight will also need laser eye protection using fast acting wide spectrum films, and self protection systems. These may include multi-spectral smoke grenades,[47] chirping ferroelectric needles that signal when an intruder steps on them,[48] miniature mines, and a multi-purpose self- protection weapon.[49] The self-protection weapon should be able to fire small and large caliber rounds, including non-lethal[50] and guided munitions.

---

[45]Arm (1992a) describes current and planned soldier-protection suits.

[46]Evancoe (1993) discusses the use of such observable reduction techniques, which he terms "metamorphic camouflage."

[47]Miltech (1994) describes a new multispectral smoke agent called NG19, able to screen visual, IR, and MMW wavelengths.

[48]Personal communication from Professor Steven Jacobsen, University of Utah Robotics Laboratory, March 1993.

[49]Personal communication from Cpt. Robert Carpenter, US Army Armament Research, Development, and Engineering Center (ARDEC), Picatinny Arsenal, November 1993.

[50]See Evancoe (1993) for a description of various types of non-lethal munitions.

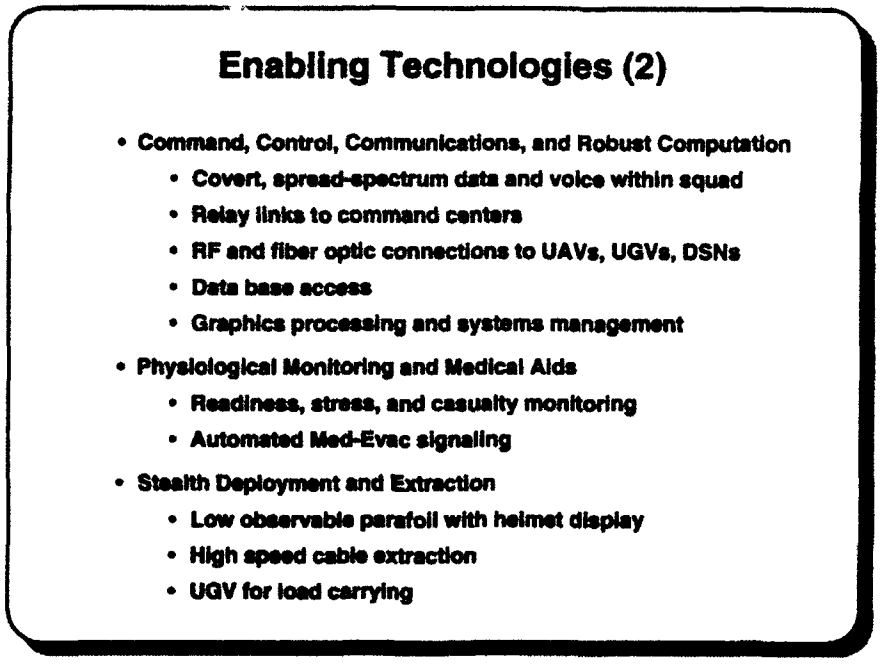
Much of the functionality of the Jedi Knight should be devoted to surveillance and sensing in the combat area. He will need night and all-weather sensing capability, with sensitive second-generation room-temperature FLIRs on his helmet (wide field of view) and weapon (narrow field of view), along with cueing from acoustic sensors able to determine both the identity and direction of vehicles, sniper fire, etc.[51] Urban warfare may similarly require a bistatic radar capable of penetrating walls and obstacles. A UAV or UGV may act as the emitter; the Jedi Knight could then have a conformal antenna on his bodysuit.

It will be useful for the Jedi Knight to have multiple sensor images displayed on his helmet screen, along with navigation and orientation data derived from GPS and from an onboard miniature IMU such as the ARPA solid state GPS guidance package.[52] He will need the capability to call for fires either by communicating target GPS coordinates or by designating the target with a combination laser ranger/designator.

---

[51]The British currently have a vehicle-mounted system called Claribel that determines the direction of sniper fire from radar antennae mounted on the four fenders (see Dewar, 1992).

[52]Aein (1993) discusses the state-of-the-art of miniature GPS-based guidance packages.



The Jedi Knight is not a lone soldier. He should be viewed as one element of an extended task force that includes command centers, intelligence operations, stand-off weapons, logistics units, and other components. Within his squad, he needs to be able to covertly communicate over distances of up to 500 meters. Selected members of the team of which he is a part should also have the capability to relay messages to satellite and UAV repeaters, communicating video images, data, requests and commands using low-probability-of-intercept systems employing millimeter-wave communications with frequencies in or near the atmospheric absorption bands.

Advances in automated systems could also allow team members to control robotic systems such as UGVs, UAVs, and mines, using RF or fiber optic command links.[53] To manage all of this, the Jedi Knight will need extremely large computational capabilities. Hardware specialists at the workshop estimated that on the order of 4000 MIPS (millions of instructions per second) will be available from small (several pound) processors in the near future; the Jedi Knight will require much of this for graphics processing and systems management.

---

[53]As one example of how such a capability might be employed, the Jedi Knight could guide a robotic device though an urban area, while at the same time accessing a structural database that shows building plans and utility maps for that area.

Physiological monitoring could be done in a largely non-intrusive manner, keeping track of such parameters as pulse, skin and core temperature, dehydration, blood loss, EEG, and even blood gases. These measurements, taken from skin sensors, micro-catheters and "radio pills" can be used to determine combat readiness, response to biological or chemical warfare, and trauma level.[54] The monitoring system should also be connected to the communication system to allow automated med-evac signaling or remote medical assistance.

To be truly effective, the Jedi Knight should be able to get in and out of the combat area covertly, using ground vehicles, helicopters, or airdrop. One insertion concept, discussed at the workshop, uses a stealth parafoil launched far from the target assembly area, with navigation and orientation information displayed on the helmet screen. Rapid extraction may have to be similarly dramatic. One approach might be to use a modified Fulton C-130 lift, with elastic cords lifting the soldier instead of the stiff line. Mobility on the ground, finally, might be aided through use of a UGV mule, which could carry such bulky equipment as radar, communications devices, remote sentries, and power supplies.[55]

---

[54]Mehregany (1993) provides a tutorial on the manufacture and use of micro-sized (a few millimeters in dimension) chemical and biomedical sensors. Brendley and Steeb (1993) describe additional applications.

[55]Muradian (1993) and (Hewish and Turbe (1991) give overviews of UGV programs now in development.

Enhancing ARPA's Research Agenda

- Current programs relevant to concept
  - Soldier Integrated Protective Ensemble System (SIPES)
  - The Enhanced Integrated Soldier System (TEISS)
  - Land Warrior
  - 21st Century Land Warrior (21CLW)
- Additional capabilities which may be required to realize Jedi Knight concept:
  - Links to robotic & MEMS devices, and bistatic sensing
  - Connections to intelligent global network
  - Long range personal weapon with guided rounds
  - Use of nonlethal weapons
  - Stealth insertion and extraction
  - Navigation using oriented helmet mounted display

Many of the components described in the Jedi Knight concept are included in programs being pursued by ARPA and the Army Battle Labs. These include the near-term SIPES and TEISS systems,[56] and the farther-term and as yet only partially defined Land Warrior and 21st Century Land Warrior programs.

We believe that research on six important capabilities needs to be enhanced to realize the revolutionary Jedi Knight concept. This includes networking the soldier into a team of robotic and manned systems, involving both micro- and macro-sized autonomous elements. This may allow special functions such as bistatic sensing, data fusion among elements, and control of smart smoke. Networking must also include connection to command centers, intelligence nodes, and databases far from the area of operations. This will require bandwidth compression, automated routing, and adaptive filtering. Depending on the mission, personal weapons should include both guided rounds and nonlethal munitions. More emphasis should be placed on insertion and extraction concepts. Display of all the information and control of all the systems and weapons, finally, should be made though panoramic helmet-mounted displays with head orientation sensing, in place of the head-up displays currently envisioned.

---

[56]See Army (1992) for a discussion of the SIPES and TEISS programs.

Overall Workshop Results: The "Bottom Line"

Promising Areas For New ARPA Initiatives

- Very Small Systems
- Biomolecular Electronics
- New Technologies For Military Logistics

An Emerging National Problem Area

(In which ARPA could play an important role)

- Cyberspace Security & Safety

A Promising Area For Enhanced ARPA Research Efforts

- Performance Enhancements for the Individual Soldier

In conclusion, four research areas have been identified as candidates for new ARPA initiatives:

- Very Small Systems
  - The use of micro and nano technologies to develop miniature (e.g., fly-size) flying and/or crawling systems capable of performing a wide variety of battlefield sensor missions.
- Biomolecular Electronics
  - The use of techniques from molecular biology and biotechnology to develop new molecular electronic materials, components, and computational architectures.
- New Technologies for Military Logistics
  - The use of modern microelectronic and information technologies as the basis for a new advanced-technology military logistic system.
- Cyberspace Security and Safety
  - The development of techniques and strategies to protect U.S. interests in and relating to "cyberspace"—the global world of internetted computers and communication systems in which more and more U.S. activities (military and civilian,

governmental and non-governmental, economic and social) are being carried out.

The first three of these represent technological opportunities for ARPA. (Of these three, New Technologies for Military Logistics is probably the most low-risk and near-term, and Biomolecular Electronics the most high-risk and far-term, with Very Small Systems somewhere in between.) The fourth area, Cyberspace Security and Safety, is an emerging national problem area in which ARPA could play an important role.

In addition, a fifth area has been identified as a candidate for enhanced ARPA research efforts:

- Performance Enhancers for the Individual Soldier
  - The use of a variety of technologies to enhance the survivability, mobility and mission performance of individual soldiers.

A. PARTICIPANTS IN WORKSHOP SESSIONS

Technology Consultants

Biotechnology & Bioengineering

Professor Robert Birge Center for Molecular Electronics Syracuse University	Biomolecular electronics and physical chemistry.
Professor Stephen Sligar Department of Biochemistry University of Illinois	Molecular biochemistry, bioorganic chemistry, and biophysics.
Mr. Robert Zimmerman Independent Consultant (Formerly Director, Biomedical Applications Program, *NASA HQ*)	Electronic instrumentation systems for biomedical research and health care delivery.

Micro & Nano Technologies

Dr. Alfred Cho[1] Director, Semiconductor Research Physics Division AT&T Bell Laboratories	Molecular beam epitaxy, quantum well devices, surface physics, crystal growth, and semiconductor device physics and performance.
Dr. Selden Crary[2] Department of Electrical Engineering & Computer Science University of Michigan	Technology of micro mechanisms & micro systems. Microflight.

[1]Attended only October 21-23, 1992 session.

[2]Attended only December 14-16, 1992 session.

Professor Stephen Jacobsen[3] Director, Center for Eng. Design College of Engineering University of Utah	Prosthetics, robotics and micro-system design.
Professor Noel MacDonald Director, School of Elec. Eng. Cornell University	Physics of micro-miniature devices, circuits, transducers & probes. Physics & device limits on the nanometer scale.
Dr. Kurt Peterson[3] Lucas Nova Sensor	Micro-electromechanical systems.
Professor Kristofer Pister Electrical Engineering Department UCLA	Silicon processing, three-dimensional silicon micro-structures, micro-robotics.

Future Information Technologies

Dr. Robert Spinrad[3] Palo Alto Research Center Xerox Corporation	Leading-edge computer science research.
Mr. Keith Uncapher[4] Center for National Research Initiatives University of Southern California	Information science, high-speed computer networking, and related technologies.

Energy Technology & Advanced Power Systems

Dr. John Bates[4] Oak Ridge National Laboratory	Advanced battery technology for small systems.

[3]Attended only October 21-23, 1992 sessions.

[4]Attended only December 14-16, 1992 session.

Dr. Robert Forward[5] Independent Consultant (Formerly Senior Scientist, Hughes Research Laboratories)	Experimental general relativity, gravitional and inertial sensors, advanced space propulsion, low-noise electronics, and space science.
Dr. Johndale Solem Los Alamos National Laboratory (Formerly Associate Head of T Division at LANL)	Atomic and nuclear physics, biology, robotics, quantum mechanics, advanced laser systems, and general weapons physics.
Mr. Harry Street[6] Sandia National Laboratory	Battery technology for small systems.

Advanced Vehicle & Propulsion Technologies

Dr. John Cashen[6] Vice President, Advanced Projects Northrop	Design of high technology systems.
Mr. Harry Scott[5] Independent Consultant (Formerly Chief Engineer for NASP, Rockwell International)	Hypersonic aerodynamics, hypersonic vehicle design, aerospace vehicle configuration design.
Mr. Robert Smith, P.E.[5] Aerospace Engineering Consultant (Formerly Vice President and Chief Scientist, Sverdrup Technology Inc., and Director of the Aeropropulsion Programs Dept. at the USAF Arnold Engineering Development Center)	Design, development, test, evaluation, and operation of gas turbine, ramjet, and solid/liquid rocket propulsion systems. Design, construction, and operation of propulsion, aerodynamic, and aerospace test facilities.

[5]Attended only the October 21-23, 1992 session.

[6]Attended only the December 14-16, 1992 session.

Autonomous Systems

Mr. Scott Harmon Hughes Research Laboratory	Military, space, and industrial mobile robots, sensor data fusion, distributed computing architectures.
Professor Dean Pomerleau Robotics Institute & School of Computer Science Carnegie Mellon University	Image understanding, computer vision, neural nets, human-computer interaction, mobile robots.
Dr. Richard Volpe[7] Robotics Systems & Advanced Computer Technology Section Jet Propulsion Laboratory	Robot computing architectures, cooperative systems, distributed planning and control, mobility systems.

Exotic Materials

Dr. David Luippold Northrop Corporation	Polymers, thin films, semiconductors, ceramics, composites, and other advanced materials

[7]Attended only October 21-23, 1992 session.

Additional Consultants & Other Outside Participants

Dr. Paul Berenson[8] Scientific Advisor U.S. Army Training & Doctrine Command	Development of military systems.
Dr. Andrew Crowson[8] U.S. Army Research Office	Technology base for military systems development.
LT COL James Dubik[8] Office, Chief of Staff Department of the Army	The future U.S. Army.
Mr. Sam Gardiner Independent Consultant	Political/military environments. Military operations (past, present and future).
Col. Randall Gressang ARPA	Development of high-technology military systems.
LT COL Robert Johnson[8] Office, Chief of Staff Department of the Army	The future U.S. Army.
Mr. Robert Moore Defense Systems & Technology, Inc.	Special operations and low-intensity conflict. Application of advanced technology to military systems.
Mr. Thomas J. Welch[9] Associate Director for S&T Office of Net Assessment, OSD	Military-technical revolution.

[8]Attended only December 14-16, 1992 session.

[9]Attended only October 21-23, 1992 session.

RAND Staff

Jack Abell
Robert Anderson
Jerry Aroesty
John Arquilla
Bruno Augenstein
Steve Bankes
James Bonomo
Chris Bowie
Keith Brendley
Glenn Buchan
Carl Builder
Edison Cesar
Terry Covington
Natalie Crawford
James Dewar
Bruce Don
George Donohue
Maury Eisenstein
Fred Frostic
Kenneth Girardini
Gene Gritton
John Halliday
Elwyn Harris
Tony Hearn
John Hiland
Kenneth Horn
Richard Hundley
Gaylord Huth
Leland Joe
Iris Kameny
Richard Kaplan
David Kassing
Rob Lempert
Jed Marti
John Matsumura
Douglas McIver
Richard Mesic
Nancy Moore
David Ochmanek
James Quinlivan
Dan Raymer
David Ronfeldt
Marv Schaffer
Russell Shaver
Calvin Shipbaugh
Ken Solomon
Rae Starr
Randall Steeb
Willis Ware
Dean Wilkening
Robert Zwirn

RAND Air Force Fellows

Lt Col Michael Anderson
Lt Col David Randle
Lt Col David Todd
Maj Tommy Garrett
Maj John Orsato
Maj David Ortiz
Maj Mark Richardson

RAND Army Fellows

LTC Kemp Littlefield
MAJ Eduardo Cardenas

TRADOC Research Associate

MAJ Gary Moody

RAND Navy Fellows

CDR Marc Goldberg
LCDR Robert Gregg

Discussion Leaders

Technology Areas at October 21-23, 1992 Session

Biotechnology & Bioengineering	Robert Birge (Syracuse) Calvin Shipbaugh Stephen Sligar (Illinois)
Micro & Nano Technologies	Keith Brendley Alfred Cho (Bell Labs) Stephen Jacobsen (Utah) Noel MacDonald (Cornell) Kristofer Pister (UCLA) Calvin Shipbaugh
Future Information Technologies	Robert Anderson Bruno Augenstein
Autonomous Systems	Dean Pomerleau (Carnegie Mellon) Randall Steeb
Exotic Materials	John Matsumura
Advanced Vehicle & Propulsion Technologies	George Donohue Dan Raymer
Energy Technology & Advanced Power Systems	Bruno Augenstein Calvin Shipbaugh

Concept Groups at October 21-23, 1992 Session

Type "A" Cases	Richard Mesic
Type "B" Cases	Fred Frostic
Type "C" Cases	Robert Moore (DST)
Type "Z" Cases	Carl Builder
"Support" Operations	David Kassing

Working Groups at December 14-16, 1992 Session

The "Fly on the Wall"	Keith Brendley Noel MacDonald (Cornell)
Turning the "Fly" into a "Wasp"	James Bonomo Fred Frostic
The "Jedi Knight"	Robert Moore (DST) Randall Steeb
The "Smart Package" & the "Smart Logistic Highway"	David Kassing Iris Kameny
"Electronic Counterfeiting" & "Embedded Agents"	Carl Builder Tony Hearn
Power Supplies for "Small" Systems	Bruno Augenstein John Hiland
Military Applications of Biotechnology	Calvin Shipbaugh Robert Zimmerman

B. POWER & ENERGY REQUIREMENTS FOR MOBILE MICROROBOTS: ORDER OF MAGNITUDE ESTIMATES

Bruno Augenstein

INTRODUCTION

This Appendix summarizes order-of-magnitude calculations of the power and energy requirements for mobile microrobots (MM) that were carried out during the ARPA workshop. These calculations led to the "base case" values cited earlier in this report of ~30 mW for hovering, ~45 mW for translational flying, and ~5 joules/km for jumping, for a 1 gram nominal MM.

In these calculations, we focus on MM in the 1 gram, 1 centimeter scale size class (wing areas for flying devices might then be in the ~1-10 cm^2 range). We view this size class as being both practically implementable early on, and producing significant utilities. Also, this class strikes some balances between "unobtrusiveness" and operational appeal.[1]

The approach we use is to make zeroth-order first principles calculations, bounded by and compared to, where applicable, parameters of insects and small birds.

As it happens, the scale size we consider lies between the smallest bird (Calypte Helenae, or the bee humming bird), with a weight ~2 grams and a wing area A_w ~5-10 cm^2, and the larger flying insects (larger in weight, size, or both), such as moths, some bees and wasps, some beetles, some dragonflies, etc., which have weights usually just under 1 gram to just under 0.1 gram and wing areas often into the ~1-10 cm^2 range. In some of these cases certain performance characteristics have been measured.

In keeping with the zeroth-order calculation spirit, we use: $g \sim 10$ meters/sec^2 and air density $\rho \sim 1$ kg/m^3—about standard air values at altitude ~2 km.

---

[1] A paper by J. Solem (1991) allowed us also to consider cases where the Reynolds number (Re) is so low that viscous effects dominate. This is <u>not</u> the case for MM of the size class we suggested for initial RDT&E; for our size class, nanotechnology is not crucially involved, and careful conventional machining, fabrication and assembly, and integration promise to carry the bulk of the RDT&E load.

ESTIMATES

The estimates presented are for hovering MM, translational MM flight, and jumping MM.

Hovering MM

The weight W is balanced, by a highly simplified momentum theorem, by an impulse $W = \rho V^2 A$, in the simplest case where the air current velocity $V/2$ through the "disk area" A furnished by rotating or oscillating wings is constant. Below the hoverer the air velocity ideally becomes V, and the flow area becomes correspondingly smaller. For the hummingbird the beating wings each cover about 1/3 the area of a disk, and the area of each wing is about 1/5 the area swept out by the wing, so that the ratio swept area/wing area ~ 5. The work L in creating the lift current is equal to the product of the lift force W and the air velocity $V/2 = V_d$ at the location of the pressure jump where the force is transmitted from the lifting disk to the air current. The specific rate of work is therefore $L/W = V_d$, in $\frac{mKg/sec}{Kg}$ units, or $L/W = V_d/75$, in hp/Kg units.

For W = 1 gm, $A_w = 5\ cm^2$ as a base case, we have a "wing loading" of $2\ Kg/m^2$, and converting to a "disk loading" appropriately we get:

$$V \sim \left(\frac{1}{\rho}\cdot\frac{2}{5}\cdot\frac{W}{A_w}\right)^{1/2} \sim 2(W/A_w)^{1/2} \sim 2(2)^{1/2} \sim 2.8\,m/sec$$

The flow velocity V_d in the plane of the disk is then ~2.8/2 ~ 1.4m/sec, and so the specific rate of work ideally is L ~ 1.4/75 ~ 0.019 hp/Kg, or ~ 14 milliwatts/gram.

The input power must accommodate losses in translation from source to wing (or propeller), in friction, in eddy formation, and so on. We estimate these losses could (probably conservatively) be a factor of 2 or so, leading to a hovering power requirement L of ~28 milliwatts/gram or, rounded, to ~30 mW/gm as a central value. Values both above and below this value are possible, by varying the areas, efficiencies, etc., but our "base case" estimate is L ~30 mW/gm. More refined estimates can be made by combining disk momentum theory and propeller theory.

For reference, note two factors:

- Data for specific power (in hp/Kg) are available for hovering flight for hummingbirds and some large flying insects. Typical values are:

  hummingbirds — ~ 0.025 to 0.035 hp/Kg
  large insects — ~ 0.012 to 0.025 hp/Kg

Considering the range of variances in weight and wing area, these are fairly satisfactory correlations.

- The value for the final air current velocity (V ~2.8 m/sec) can be compared with the average human measurements for open mouth breathing and pursed mouth blowing, measured a few centimeters from the mouth:

  breathing — ~ 2 m/sec
  blowing — ~ 20 m/sec

  From this we see that values for the hovering air currents for hummingbirds, our MM, and large insects correspond roughly to open mouth breathing currents, and are rather modest.

Translational MM Flight

The simplest case here is just to "tilt" the MM used in the hovering calculation, so as to produce both a lifting and translational force. When these are roughly equal, the power needed is ~ 45 mW/gm, if we need ~30 mW to support our 1 gram MM.

This is not wholly satisfactory because we want to have a range of speeds available, and we want to be able to exploit properly the aerodynamics of airfoils. As we will see, this is possible at fairly good values of translational speed V_t with required powers still of the order of ~45 mW/gm. We assume a propeller-driven MM.

It is easy to show that for level, unaccelerated flight these relations hold:

$$\text{Power} = \left(2W^3 C_D^2 / \rho A_W C_L^3\right)^{1/2}$$

$$V_t = \left(2W / \rho A_W C_L\right)^{1/2}$$

where W = weight, C_D = drag coefficient, and C_L = lift coefficient.

Note that the minimum power P (and hence also the maximum endurance) is attained at the maximum value of $C_L^{3/2} / C_D$. In contrast, maximum range is attained when C_L/C_D or L/D is maximized. All of this is analytically trivial when we have the ideal parabolic drag polar (C_L, C_D relation) for airfoils. In that case, it is easy to show that the L/D for maximum endurance, or minimum power—(L/D_E)—is $\sqrt{3}/2$ the L/D for maximum range—(L/D_R)—so that (L/D_E) ~ 0.87 (L/D_R). Also, the flight speed for maximum endurance is ~$3^{-1/4}$ ~ 0.76 the flight speed for maximum range.

At the Reynolds number (Re) we are concerned with (i.e., Re of the order of roughly 10^4), measurements on thin wings, slightly arched, with aspect ratios in

the range ~1 to 5, and roughly the size of small hummingbird wings or large dragonfly wings, suggest the following ranges of values are realistically obtainable:

Maximum values of CL ~ 0.5 to 0.9

Maximum values of L/D ~ 3 to 6.5.

We thus have a range of values available for A_W (i.e., our spread of ~1-10 cm^2), and for C_L and C_D. A choice reflects what we might want to optimize—e.g., let us optimize endurance (minimum power).

Then, for example, we might be content with "conservative" combinations such as $A_W \sim 5\ cm^2$, $C_L \sim 0.60$, $C_D \sim 0.16$, for which the ideal power P ~ 22 mW, which with overall efficiencies of ~1/2 translates into a required power of P ~ 45 mW. The flight speed V_t is then $V_t \sim 8$ meters/sec. Or we could fly faster, easily twice as fast (to, say, ~ 16 meters/sec), by using somewhat smaller A_W and/or smaller C_L—but at the expense of increased power.

For reference, the maximum speed of hummingbirds is of the order of 20-25 meters/sec, and that of the largest dragonflies is of the order of 15 meters/sec, so again the MM seems to have values of a reasonable order of magnitude.

Jumping MM Translation

It is useful and convenient to treat jumping translational motion somewhat differently from flight. Energy factors in jumping include the energy needed for pure ballistic flight—and three other factors: energy losses from the energy source to the jumping mechanism, energy losses due to drag while in motion, and the possibility of elastic energy reconstitution during landing and subsequent jump. For a zeroth-order analysis we can assume the last three factors to compensate for each other, so that to this approximation we need consider only the ballistic flight.

Within this approximation we can assume launching the jumper at speed V and at an angle ϕ of about 45°, so that:

t = time of flight ~$1.4V/g$
R = range of flight ~V^2/g
h = maximum elevation ~$V^2/4g$

We can set h at some nominal value to generally clear obstacles; say we put h = 1 meter as a base case. Then we get:

$V \sim (4gh)^{1/2} \sim 6.3$ meters/sec
t ~ 0.9 seconds
R ~ 4 meters

From this, it takes N ~ 250 jumps to go 1 kilometer, and the energy, E, expended for 1 kilometer of jumping of a 1 gram MM, under our approximations, is just:

$$E \sim N(mV^2/2) \sim 5 \text{ joules.}$$

Within this approximation the energy required to jump 1 kilometer with $\phi = 45°$ is independent of the particular choice of the associated h, V, and R. However, practical problems of jumping and the associated mechanisms probably make it convenient to jump in relatively small steps. Jumping mechanisms and any elastic reconstitutive mechanisms, together with stability problems, and so on, may make jumpers initially more challenging MM than flyers. Combining flying and jumping attributes in the same system may have control, stability, and performance merits. The insect world has many examples of pure jumpers and combined jumper/flyers.

DISCUSSION

These estimates can be made more refined, in obvious ways, but this is properly done in the context of a combined design and experimental program. The point of these zeroth-order estimates is to suggest that satisfying the basic energy needs seems reasonably promising, and that some "safety factor" assumptions are present.

The estimates made might well be on the conservative side, and there seem to be large tradeoff opportunities. For example, while it seems attractively possible for our 1 gram , 1 centimeter scale size MM to fly, say several tens of kilometers, using power from a class of batteries storing ~1.6 kilojoules per gram, it should be recalled that sensors or other loads plus communications and navigation plus stabilization needs also consume power. Integrating structure, power, and performance aids in a 1 gram, 1 centimeter scale size package doing useful jobs seems possible, challenging, and worthy of significant RDT&E.

Comparisons to the performance and mechanical designs of the natural world suggest a number of goals worth trying to achieve. Just three examples (out of many) are:

- The flight capabilities of a hummingbird are exceptional and rely on, among other things, wonderful articulations in the wing structure. Hummingbird hovering performance is unsurpassed (hummingbirds can also fly upside down, backwards, and in other bizarre translational modes), and yet the bird is also capable of forward speeds of ~20 meters/sec, or about 200-400 body lengths per second. Trying to mimic such performance even approximately in MM would be, to say the least, an enormous challenge.
- The wings of many insects are marvels of ultralight construction. For example, the wing of the adult blue dragonfly is ~ 5 cm long and ~ 5 cm^2 in area and weighs ~ 5 milligrams. The thin membrane (the vast majority of the wing area) behind the main "wing girder" is ~ 3 microns thick and weighs about 3.7 grams per square meter. These wings are strong enough to beat 20-40 strokes per second and support a dragonfly weighing of the

order of ~ 10^{-1} grams at forward flight speeds of the order of 15 meters per second.

- A typical locust has a folding wing (folding into pleats) which allows it to effectively combine jumping and flying. This folding wing is about the same size as the blue dragonfly wing, and yet weighs only about 50 percent more than a non-foldable wing.

All in all, planning and execution of a competent MM program in the ~ 1 gram, ~ 1 cm scale size range should present enough opportunities and possible operational returns to attract a critical mass of expert researchers.

BIBLIOGRAPHY

(Aein, 1992) Joesph M. Aein, *Miniature Guidance Technology Based on the Global Positioning System*, RAND, R-4087-DARPA, 1992.

(Aoki et al., 1992) Takafumi Aoki, Michitaka Kameyama, and Tatsuo Higuchi, "Interconnection-Free Biomolecular Computing," *Computer*, Vol. 25, No. 11, November 1992, pp. 41-50.

(Army, 1992) *Army Technology Base Master Plan*, Headquarters, Department of the Army, Deputy Assistant Secretary for Research and Technology (SARD-ZT), February 1992.

(Army, 1992a) "Army Weaponry and Equipment," *ARMY*, October 1992.

(Birge, 1992) Robert R. Birge, "Protein-Based Optical Computing and Memories," *Computer*, Vol. 25, No. 11, November 1992, pp. 56-67.

(Birge and Gross, 1992) Robert R. Birge and Richard B. Gross, *Biomolecular Optoelectronics*, Center for Molecular Electronics, Syracuse University, Syracuse, New York, 1992.

(Brendley and Steeb, 1993) Keith W. Brendley and Randall Steeb, *Military Applications of Microelectromechanical Systems*, RAND, MR-175-OSD/AF/A, 1993.

(Capstick et al., 1992) Myles H. Capstick, W. P. Liam Marnane, and Ronald Pethig, "Biologic Computational Building Blocks," *Computer*, Vol. 25, No. 11, November 1992, pp. 22-29.

(Chan and Dill, 1993) Hue Sun Chan and Ken A. Dill, "The Protein Folding Problem," *Physics Today*, Vol. 46, No. 2, February 1993, pp. 24-32.

(Chen and Birge, 1992) Zhongping Chen and Robert R. Birge, *Protein Based Artificial Retinas*, Center for Molecular Electronics, Syracuse University and Biological Components Corporation, Syracuse, New York, 1992.

(Cho, 1988) Alfred Y. Cho, "Artifically Structured Materials," in Anthony P. French (ed.), *Physics in a Technological World*, American Institute of Physics, 1988, pp. 163-175 .

(Conrad, 1992a) Michael Conrad, "Molecular Computing Paradigms," *Computer*, Vol. 25, No. 11, November 1992, pp. 6-9.

(Conrad, 1992b) Michael Conrad, "Molecular Computing: The Lock-Key Paradigm," *Computer*, Vol. 25, No. 11, November 1992, pp. 11-20.

(Crary et al., 1992) Selden B. Crary, G. K. Ananthasuresh, and Sridhar Kota, "Prospects for Microflight Using Micromechanisms," *Proceedings of the International Symposium on Theory of Machines and Mechanisms*, Nagoya, Japan, September 1992.

(Dewar, 1992) Michael Dewar, *War in the Streets; The Story of Urban Combat from Calais to Khafji*, David and Charles, Newton Abbott, UK, 1992.

(Evencoe, 1993) Paul Evencoe, "Non-Lethal Technologies Enhance Warrior's Punch," *National DEFENSE*, December 1993, pp. 26-29.

(Feynman, 1959) Richard Feynman, "There's Plenty of Room at the Bottom," American Physical Society annual meeting, Pasadena, California, December 29, 1959; published in *Engineering and Science*, California Institute of Technology, February 1960; excerpts reprinted in *Science*, Vol. 254, pp. 1300-1301, 29 November 1991.

(Gardner and Hingle, 1991) J. W. Gardner and H. T. Hingle (ed.), *From Instrumentation to Nanotechnology, Developments in Nanotechnology*, Vol. 1, Gordon and Breach, Science Publishers, New York, 1991.

(Hameroff et al., 1992) Stuart R. Hameroff, Judith E. Dayhoff, Rafael Lahoz-Beltra, Alexei V. Samsonovich, and Steen Rasmussen, "Models for Molecular Computation: Conformational Automata in the Cytoskeleton," *Computer*, Vol. 25, No. 11, November 1992, pp. 30-39.

(Hewish and Turbe, 1991) Mark Hewish and Gerard Turbe, "Europe and US pursue battlefield robotics," *International Defense Review*, January 1991, pp. 40-47.

(MacDonald, 1992) N. C. MacDonald, *Single Crystal Silicon Nanomechanisms for Scanned-Probe Device Arrays*, IEEE Solid-State Sensor and Actuator Workshop, Hilton Head Island, South Carolina, June 22-25, 1992.

(Mehregany, 1993) Mehran Mehregany, Wen H. Ko, Andrew S. Dewa, and Chung-Chium Liu, *Introduction to Microelectromechanical Systems and the Multiuser MEMS Processes, Part I: MEMS Overview; Chapter 4. Chemical and Biomedical Sensors*, Case Western Reserve University—MCNC Short Course, August 8-10, 1993.

(Miltech, 1994) "Industrial Focus: NICO Smoke Screen," *Military Technology*, February 1994, p. 26.

(Muradian, 1993) Vago Muradian, "Unmanned Vehicles: Military Missions Multiply for Robots," *Defense News*, September 20-26, 1993, p. 12.

(Rambidi, 1992) Nikolay G. Rambidi, "An Approach to Computional Complexity: Nondiscrete Biomolecular Computing," *Computer*, Vol. 25, No. 11, November 1992, pp. 51-54.

(Sligar and Salemme, 1992) Stephen G. Sligar and F. Raymond Salemme, "Protein engineering for molecular electronics," *Current Opinion in Biotechnology*, Vol. 3, 1992, pp. 388-394.

(Solem, 1991) Johndale C. Solem, *On the Motility of Military Microrobots*, Los Alamos National Laboratory, Report No. LA-12133, July 1991.

(Whitehouse and Kawata, 1990) D. J. Whitehouse and K. Kawata (eds.), *Nanotechnology: Advances in Nanoscale Physics, Electronics, and Engineering*, Proceedings of the Joint Forum/ERATO Symposium held at Warwick University, 23-24 August 1990, Adam Hilger, 1990.

(Whitesides et al., 1991) George M. Whitesides, John P. Mathias, and Christopher T. Seto, "Molecular Self-Assembly and Nanochemistry: A Chemical Strategy for the Synthesis of Nanostructure," *Science*, Vol. 254, 29 November 1991, pp. 1312-1318.