Preprint
UCRL-JC-141358

After Globalization Future Security In A Technology Rich World

T.J. Gilmartin

This article was submitted to
After Globalization Future Security in a Technology Rich World
Livermore, CA
December 13-14, 2000

U.S. Department of Energy

Lawrence
Livermore
National
Laboratory

February 12, 2000

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint is made available with the understanding that it will not be cited or reproduced without the permission of the author.

This report has been reproduced
directly from the best available copy.

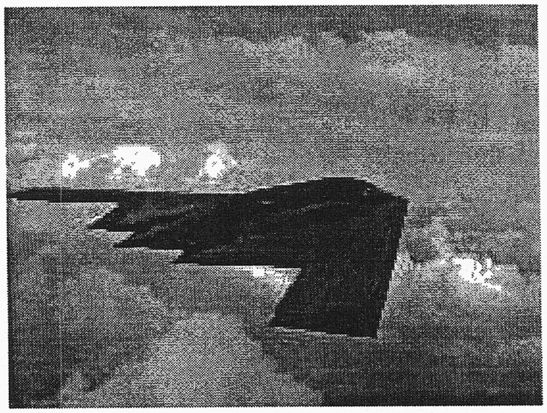
Available to DOE and DOE contractors from the
Office of Scientific and Technical Information
P.O. Box 62, Oak Ridge, TN 37831
Prices available from (423) 576-8401
http://apollo.osti.gov/bridge/

Available to the public from the
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd.,
Springfield, VA 22161
http://www.ntis.gov/

OR

Lawrence Livermore National Laboratory
Technical Information Department's Digital Library
http://www.llnl.gov/tid/Library.html

After Globalization
Future Security in a Technology Rich World



Center for Global Security Research
Futures Project
2000

Project Report
February 12, 2000

AFTER GLOBALIZATION: FUTURE SECURITY IN A TECHNOLOGY RICH WORLD

Over the course of the year 2000, five one-day workshops were conducted by the Center for Global Security Research at the Lawrence Livermore National Laboratory on threats that might come against the US and its allies in the 2015 to 2020 timeframe due to the global availability of advanced technology. These workshops focused on threats that are enabled by nuclear, missile, and space technology; military technology; information technology; bio technology; and geo systems technology. In December, an Integration Workshop and Senior Review before national leaders and experts were held

The participants and reviewers were invited from the DOE National Laboratories, the DOD Services, OSD, DTRA, and DARPA, the DOS, NASA, Congressional technical staff, the intelligence community, universities and university study centers, think tanks, consultants on national security issues, and private industry.

For each workshop the process of analysis involved identification and prioritization of the participants' perceived most severe threat scenarios (worst nightmares), discussion of the technologies which enabled those threats, and ranking of the technologies' threat potentials. We were not concerned in this exercise with defining responses, although our assessment of each threat's severity included consideration of the ease or difficulty with which it might be countered.

At the concluding Integration Workshop and Senior Panel Review, we brought the various workshops' participants together, added senior participant/reviewers with broad experience and responsibility, and discussed the workshop findings to determine what is most certain, and uncertain, and what might be needed to resolve our uncertainties. . This document reports the consensus and important variations of both the reviewers and the participants.

Contents

MAJOR CONCLUSIONS

In all, 45 threats over a wide range of lethality and probability of occurrence were identified. Over 60 enabling technologies were also discussed. These are each described in greater detail in the following pages, after overarching considerations are discussed. Here we present the major conclusions of this project, which each include consideration of several threats and their enabling technologies.

MAJ-1. TERRORIST NUCLEAR WEAPON

The danger that terrorists might use a crude or procured nuclear weapon to attack a city is non-negligible. The proliferation of nuclear weapons, the atrophying of huge cold war stockpiles, the global increase generally in nuclear technology, the rising tide of all non-nuclear enabling technologies, from computing to robotics to remote control, and the ease of covert delivery, all increase the probability that a nuclear weapon will become available to and be used by a highly motivated agent. Attribution of such an attack may be difficult if the sponsoring group decides not to claim responsibility, and such extreme terrorism might be viewed as useful by a number of hyper-zealous organizations.

MAJ-4. NATURAL AND ENGINEERED DISEASE

Unfortunately, diseases eliminated or controlled in public still exist in biological storage, are known to persist in relatively isolated populations, or are reemerging in drug resistant forms. Much of the once immunized population is again vulnerable, for example, to smallpox and to antibiotic resistant tuberculosis. In addition, new diseases are emerging, and biotechnology is now able to modify and combine disease elements to tailor their effects and potentially even to select their targets by racial or ethnic identity. Bio regulator technology, which can alter human function and performance, is increasingly sophisticated and available, for both beneficial and malicious uses. The technology, production means, and dispersal mechanisms needed to initiate a bio-attack are simple and difficult to detect, and the knowledge of how to accomplish these ends is widespread. The potential for serious mischief along these lines is great.

MAJ-2. LIMITED NUCLEAR WAR

Ironically, the technological obsolescence of legacy military technology and the revolution in military technology is favoring the nuclearization of emerging powers, which cannot afford and are unable to implement competitive sophisticated systems-of-systems forces. Nuclear weapons give immediate dominance over or nuclear peerage with local adversaries, deterrent capability in preconflict calculations and in conflict operations, and to-be-reckoned-with stature among world powers. Examples are Israel, India, and Pakistan, and potentially Iraq, Iran, DPRK, and others during the next two decades. The asymmetries between these nations and their adversaries make mutual understandings difficult; and the intensity of feelings prevents dialogue and minimizes restraint.

It is certainly possible, and maybe even likely that some such situation will result in the use of such weapons, out of desperation or vengeance, or in an EMP mode, this being less provocative but militarily effective. Such localized use of nuclear weapons would reinforce the rationale for emerging nations to have such weapons and probably would increase proliferation and global risk.

MAJ-3. MAJOR NUCLEAR WAR

While it is generally thought or hoped that the threat of global nuclear war has receded, massive arsenals and delivery capabilities still exist, are growing in some cases, and are imbedded in a more complex geopolitical matrix. This situation might be more analogous to the multifaceted relations prior to World War I than to the bipolar Cold War stand-off, with now an array of powerfully armed nations and a second tier of emerging nuclear actors with intense animosities and a range of alliances with each other and with the primary nuclear powers. This system is very nonlinear, not stable, and far more difficult to crisis manage, if only because the scenarios are many, the interactors diverse, and the management protocols undefined and untried. This threat ranks high not based on any current tension, but because of the uncertainties and the portential for catastrophe.

MAJ-5. HUMAN CONTROL OF BIO FORMS

In addition to the malicious applications of biotechnology listed above, the fact that humanity is increasingly able to design and make new bio forms, from viruses and proteins (and prions) to bacteria to flora and fauna, is both wonderful and frightening. Evolution has constructed the microorganisms and biota of today over very long periods and has tested extremely complex interrelationships such that species are in equilibrium with their environments. Most of man's biological creations will serve specific purposes, such as, manufacturing medicines and organs for human use, and improving the productivity and performance of species, even of humans. These improvements will not be ecologically tested; such testing would be extremely complex, if possible at all. In fact, the ease of biological creation will enable recreational genetics and bio hacking. The dangers of ecological and human disruptions will be great. In addition, nano technology and molecular scale information technology will blur the boundary between biology and heretofore inorganic technology. To quote one project participant, "It will be a brave new world when man controls evolution and the worlds of carbon and silicon converge." All of these activities are already ongoing.

MAJ-6. US FORCE PROJECTION COUNTERED

Stealth, anti-aircraft IR and radar counter measures, AWACS, and IR sensors and guidance have given the US dominance and near impunity in projecting air power. An array of new air defense and air combat technologies threatens not only to compromise this dominance, but to push farther back from the combat areas our forward projection air and sea support systems. These technologies include: IR focal plane array (IRFPA) sensors, which might defeat IR countermeasures; conformal IR missile dome optics, which give anti-aircraft missiles greater speed and range; IR search and track (IRST) systems, and low frequency, multistatic, and expendable radar systems, which lessen the effectiveness of stealth and anti-radar missiles; and airborne or space based radar, IR, and visible sensors, specifically moving target indication (MTI) systems, which also lessen the effectiveness of stealth and of US cruise missiles. Add to this that stealth technology will become available for adversaries' aircraft, missiles, and ships, which will require greater standoff and other protections for our aircraft carriers and AWACS, and that improved IR systems will increase adversaries' night operational effectiveness. The result will be diminished US air dominance and forward strike capability, the necessity of US forces to "share the night," and the need for a new generation of strike and countermeasure technologies.

MAJ-7. CONTROL AND LOSS OF CONTROL OF NATURE

On the one hand, we are gaining greater control of natural phenomena. Models of global atmosphere/ocean/biosphere physics are being coupled to mesoscale and regional models, potentially enabling more accurate prediction and even, speculatively, some degree of control of weather and climate. This capability would be of great national advantage. Similarly, the understanding of tzunami generation by undersea continental shelf slump and landslide, and methane release from metastable undersea clathrate formations are both potentially triggerable events.

On the other hand, human activities are changing atmospheric composition, adding green house gases and depleting ozone, which can change the global environment in ways that we are not as yet able to control. The effects of these changes are predictably distributed, with much variation of benefit and harm among regions and nations. Our inability to control these effects is very troubling and their actual distribution, when known, is certain to be a source of international antagonism. These effects on the US homeland are, on balance, significantly negative.

MAJ-8. DRAINING INFORMATION WARFARE

The number and variety of information operations that might be used against the US occupied much of our discussion, from simple civil intrusion and denial of service to complex tapestries of financial, infrastructure, and military system attacks. Such attacks during the year 2000 disabled Internet services and undoubtedly cost considerable money. However, although the frequency of lower level but costly mischief attacks will increase, and our information infrastructure will require constant defensive modifications to continue to function effectively, it was judged that defenses would evolve as needed and that such attacks would not ultimately threaten either the US sovereignty, economy, or military dominance. With adequate wariness and prudent precautions, we should be able to prevent or contain financial losses, disinformation, security breaches, system intrusions, and infrastructure attacks. In fact, the more complex the planned assault, the more probable its detection and avoidance.

MAJ-9. PAINFUL ASYMMETRY

US military dominance is a very positive example of asymmetry. It is highly unlikely during the next two decades that any adversary will defeat us in conventional conflict. In fact, our military effectiveness might be increased by adopting techniques currently regarded as asymmetric.

But, US concentrations of value (people, cities, infrastructure, industry, energy supplies, embassies, ships in port,...) are prodigious and vulnerable. It is repeated everyday in new reports that we are not properly organized, trained, equipped, or positioned to prevent devastating attacks on these sorts of targets.

While our discussions did repeatedly reveal new vulnerabilities to such attacks and new methods for such attacks, and did decry the commonly identified deficiencies in US organizational responsibility and capability, it was also agreed that such attacks would not seriously threaten the US military or government, and that most perpetrators would eventually account for their actions. This is not to downplay the nature and difficulty of dealing with today's asymmetries, but to keep such potential actions in perspective.

Acute intelligence, mutual international commitments and collaborations, special forces, and clear responsibility for homeland defense and emergency response were all offered as necessary responses to asymmetric threats.

OVERARCHING CONSIDERATIONS

The threats discussed during this project have ranged from site-specific to global, from intentional to natural, from economic to massively destructive, and from personal to governmental. The responses to these threats range from technological to social and diplomatic. We will begin below with a contextual discussion of threat and response types.

In addition, several overarching threat themes not specific to a technology sector have emerged. These include globalization effects per se; failure of our defense forces to adapt to future missions and technology; disruptions of vital resources, ecosystems, and the global environment; and socio-political threats to our Republic. These overarching themes are complicated, having both positive and negative aspects that derive from the same root causes. Again, our discussion of these themes below is intended as contextual.

GLB-1. THREAT TYPES

Traditional or New.

Some threats treated in the following pages, such as information, geo-system, and biological threats, are quite open ended at this time. These are based on emerging knowledge and technology, which are only beginning to be realized. Our assumptions about future technological capabilities, such as, an almost information transparent and accessible world, man-designed organisms , and large-scale natural phenomena that might be predictable, even controllable, are still speculative. These speculations allow us to conceive almost "science-fiction" threat scenarios, not based in past experience, and frightening as much because they are unknown, as because they will actually turn out to be destructive.

We think that we understand nuclear weapons and are more comfortable discussing the strategies and defenses that we have used for 55 years. In fact, the nuclear threats have become more complex, such that our traditional analytic methods and theories of deterrence are no longer adequate. Nuclear threats are more new than traditional.

New sensors, networked systems, high-performance air and sea vehicles, and missile and even space technology, although very challenging, as in the case of stealth and infrared focal plane sensor arrays for anti-aircraft missiles, are seen as more traditional threats that technology can defeat.

Dangers to the fabric of our society caused by any of the threats above came up in all of our discussions, are historical, although newly enabled by revolutionary technologies, and are discussed briefly below (GBL-6).

Intentional Massively Globally Destructive.

Our attention has been focused on the worst threats that arise from intentional acts, using weapons of mass destruction, or threatening global assets or conditions. Intentionality calls for deterrent measures and commensurate response capability, and demands the most attention in terms of analysis, force design and implementation, international engagement, and expenditure.

Intentional Limited.

This category includes for the most part traditional military and now terrorist threats and derives from military capabilities. This is the threat set that our military and civilian authorities are designed to deter, control, and counter. Expenditure is greatest against this threat set.

Unintended Man-made.

This is a very frightening set of threats, from the consequences of global warming to the long-term results of life-form modifications, bio-diversity and habitat loss, and the socio-political transformations driven by information technology. All of these threats derive from man-made benefits; but man has proven many times to have limited foresight, and even ignorant hindsight, when exercising his stewardship.

Natural.

Some natural disasters could come under man's influence (storms, tsunamis, earthquakes) or even control (emerging diseases, asteroid impacts) due to technological advances. These are deserving of continued analysis and research. However, watchfulness and emergency preparedness and response comprise what we can do with these threats at this time.

GLB-2. RESPONSE TYPES

Development of the responses to the threats discussed herein is outside the scope of this project, and might be the goal of follow-on projects. We have done this because, in our experience, a response focus can capture the minds of the participants and limit their threat imagination, and because the discussion of threats and enabling technologies alone is a prodigious scope. However, some general discussion of responses helps to set the context for the threat discussion.

Technological and Scientific.

Would that all threats had technological responses. Indeed, as the threats are better defined and as technology advances, some of the threats will be controllable by technical means. We might learn how to contain emerging diseases and thereby counter intentional disease-based threats. We might develop effective missile defense and large-area nuclear device detectors. We will improve the security of the networks; this is happening. We might increase our control over natural disasters. We will improve the technical effectiveness of our military forces; the question here is, to what extent others will avail themselves of the same globally available technological advantages.

National.

We will try to develop our military forces and civilian authorities such that they might deter, prevent, counter, and respond to the threats that are judged most lethal and probable to harm us. This is a mixture of technological, cultural, and authoritarian responses. War, terrorism, and crime might be contained by these measures. Informational, biological, and environmental threats are evolving, and are not yet contained by these traditional responses, but will require governance, as well as technological solutions.

International.

To date, international agreements (STARTs, NPT, BTWC , CWC,...) to limit international threats from nuclear, biological, and chemical weapons, from disease, from crime, and from inhumane actions have been designed to guide national actions, not to force them. National sovereignty has been the norm; international governance has been the exception. UN "police" actions, IAEA inspections, ISO standards, and IMF rules, for examples, indicate a trend toward more global governance, and potentially more global options for response to some of the threats considered here.

Declaratory Policy.

In addition to military and national preparation, and international agreements, an effective overall response strategy is declared and understood, with credible exchange calculations, and the effected parties understanding each other's intentions and having common ground for evaluating the outcomes. Even a technological response requires some declaration of intention to achieve its full effect, that is, both the deterrent and physical effects.

In retrospect, we regard the nuclear weapon standoff and agreements between the US and the USSR as informed and rational, based on calculations, common understanding, and similar ultimate values. We are now concerned that India and Pakistan are miscalculating, do not understand each other's assumptions, and are unable to define shared values. Similarly, in general, for the Islamic and Western worlds, each culture considering that the other is irrational. This stumbling block substantially degrades the efficacy of any responses to mutual threats.

GLB-3. GLOBALIZATION

Technological globalization is the context for our consideration of future threats, that is, the assumption that many nations will become technologically sophisticated, and will become wealthy and significant world players thereby, and that weapons capabilities and sources, even for the US, will be globally distributed. Globalization per se might cause threats to US stability and advantage.

Marketization.

In contrast to the just past period of ideological motivation and conflict, marketization is pervading even insistently socialist economies like China and now nominally North Korea. This requires greater openness and commitment to international interdependence, acceptance of economic power as an alternative to military might, and a willingness to engage in private capitalization on a scale that can dwarf government resources. It is characterized by a backing away from centralized control, in fact from any causal control, away from nationalization, even from regulation, in the belief that the "invisible hand" will provide beneficial guidance and not itself become the next tyrant.

While the free market has enabled US success and prosperity, the market is less able to enlighten and manage several threatening trends, namely, the power of drug cartels, the emergence of international crime syndicates, the advantage taken of workers with little voice in the market, local environmental damage, the loss of habitat and environmental heritage, and the global environmental effects of global production and energy use. These problem situations can threaten the US in the short and long terms.

Denationalization.

In the San Francisco Bay Area, the information economy dominates all other business sectors by an order of magnitude. This economy is staffed by workers, who are not US citizens in the majority, who often do not reside in the US, and who migrate dynamically to the information action centers of the world. These workers are educated in once indigenous universities, now international, often not in their own country. Information products and capital flow across national borders almost as though these boundaries did not exist. This is true of the automotive industry, pharmaceuticals, space launch, military hardware, and agricultural products. The markets and means of production are global entities and dynamic in their hybrid nationalities.

On the one hand, denationalization has enabled unprecedented prosperity and international commercial integration. On the other, the US has substantially less control over the distribution of critical technologies, the protection of intellectual property, the flow and quality of capital, goods, and services, the movement of people (and their intellectual value), and the actions of non-national groups and organizations. This is not internationalization (interaction among nations), but is denationalization, which is the growth of groups, organizations, and activities that do not value or even recognize national sovereignty.

Since the US is globally dominant by almost any measure, the diminishment of national boundaries can work to our advantage, giving us greater access to foreign markets, resources, and information; but this openness also creates reciprocal vulnerabilities from those who want our economic resources or want to harm us.

Disinfrastructurization.

Systems of systems have been the hallmark and a dominant advantage of the US military. These systems were provided by a military industrial complex that is no longer captive to the US military, and no longer nationally definable. Many of the systems upon which the military depends are commercial, from space and communication systems to basic infrastructure and computer hardware and software. In fact, there are highly developed commercial analogs for most functions of military systems of systems: hardware, strategy, doctrine, training, logistics, and movement. The COTS systems of systems are inter- and intra-integrated without military specifications, and available to all customers. In so far as these are used, the US military systems of systems will be less militarily specific and will be more available to adversaries, and may in fact have been partially built by them. If the US does use the most current technology, this technology will necessarily be more commercial, more accessible to adversaries, and more vulnerable to mischief.

Disinfrastructurization, that is, the production and integration of systems by virtual suppliers, using disparate, other-owned, even anonymous suppliers, just in time, is the current commercial production model. There is much less end-product-dedicated supplier base for any products, and in particular, much less military industrial supplier base. Highly integrated systems are agilely manufactured from the most advanced interoperable technologies, commercially available from distributed indigenous sources, not readily tracked or even completely attributable, because the production complex is virtual, ad hoc, very complex, and not overtly military. This production mode further decreases US control over technology sources and increases adversary invisibility and access in obtaining advanced technology systems.

Anti-Globalization

No matter where the World Trade Organization, or the International Monetary Fund, or the World Bank has met over the last several years, the meetings have been surrounded by protests, some violent. The protestors represent international groups dedicated to human rights, environmental issues, defense of the Third World, anti-capitalism, anti-business, anti-world organization, anti-US hegemony, and various other viewpoints across the ideological and political spectrums, some profound and visionary, some anarchistic and revolutionary. These non-governmental affinity groups are one element of the denationalization mentioned above.

Organized over the Internet, both strategically and specifically, in real time for the purpose of the protests, these groups use the advantages afforded by freedom of speech, the tactics of information operations for conflict and disruption in cyber space, and physical violence, some being law-abiding, but others being radical, revolutionary, and anarchistic.

This trend can escalate to terrorism. Particularly as zealous defenders of a range of Earth's assets and resources are frustrated by their apparent inability to deal with global unsustainability and the disparity of wealth, discussed below, their spectrum of methods could widen. These movements could also use the opportunities of other attacks on the global economic infrastructure and particularly that of the US to add their own movements.

Clearly, we all benefit from the clarion voices of visionaries and of those who care above themselves for global well being. Unfortunately, some are excessive and, given the lethality of modern technology, potentially very harmful.

GLB-4. RISK TO OUR MILITARY

Tomorrow's War

There is no doubt that the US will have to plan to fight conventional force-on-force warfare and to maintain a substantial nuclear deterrent. However, it is difficult to imagine a major theater war with a major, or even minor, nuclear power; it is hoped that nuclear war can be avoided by layered precautions and sufficient direct engagement; and it is unlikely that a lesser power will be willing to engage the US directly in a war between conventional forces, although surrogates (states, guerillas, and terrorists) might be used in limited fashion. Thus, substantial scale conventional and nuclear US forces must be kept, but success will be that neither of these forces is used at scale.

Both the Persian Gulf and Serbian conflicts emphasized information, air dominance, precision, and remote strike advantages in a limited conflict. As globalization provides some of these advantages in at least asymmetric fashion to adversaries, and if nuclear weapon capabilities proliferate further, limited actions among nuclear capable states could become more likely and the application of US conventional advantages would become more complicated. In future localized conflicts, dominance and security of information and space assets, as well as control of the contested air and sea, must continue to be quick and complete for the US, although these may be seriously contested. Theater and point missile defense will be increasingly critical, and increasingly more difficult, as adversaries learn to avoid and deceive our sensors

The defense of our cities and infrastructure, and of our own electronic assets is a whole new responsibility and faces a rapidly emerging ensemble of challenges. Secretary Cohen, speaking at the Center for Strategic and International Studies, pointed out that this responsibility is not well defined. It is clear that our military forces lack some of the specific capabilities, and the mission, needed for asymmetric conflict and homeland defense. It is likely that highly coordinated defensive "forces" including the US military, international forces, law enforcement, civilian government and industry, and the media would be needed. We are not prepared or practiced for this sort of tapestry defense and tapestry conflict. John Hamre said that the US military can go anywhere in the world and defeat any foe, singly or in combination, but lacks the ability to save 10,000 Americans exposed to a terrorist WMD weapon, calling into question our concept of defense.

Command

It is likely that future defense forces will be assembled in real time around specific threats, with command structures that are more ad hoc, autonomous, and networked. This form of organization, rapidly formed and reformed, is common in business and society today, but it is antithetical to military hierarchy and military information rigidity. We could fail to dominate an unpredictable, agile adversary, if our command structure and our command technology are less agile, and if we are not prepared to confront very unconventional, asymmetric situations, such as indigenous (Vietnam, Somalia), urban, and cyber warfare.

Tradition and Legacy

Service roles and systems should also be adaptable to virtual coordination and almost continual renewal, even in real time, as threats evolve and our experience with them grows. Beyond joint operations, we will need to decentralize command and operations among our forces, and to integrate diverse systems and organizations. This is possible to only a limited extent with traditional military roles and legacy systems. Our goal must be truly integrated, unified forces and systems, and the capability to coopt non-military resources.

New Vulnerabilities

As technology globalizes and advances, our aircraft, aircraft carriers, submarines, space assets, information systems, and ground forces will face new threats. For example, rapidly proliferating infrared imaging technology threatens one of our core advantages in the battlefield - the boast that "we own the night". The same technology introduces a new level of threat against our combat aircraft and our flexibility to "own the air" over enemy territory and to attack their ground forces with near impunity. The threat to ground navigation systems is illustrated by a recent event in which France tampered with a GPS signal to disadvantage a competing British tank demonstration. The combination of stealth and improved cruise missile performance will threaten our carriers and push them farther away from the adversary's space. As we learned in Kosovo and Serbia, the use of deception and decoys, concealment, disinformation, and electronic countermeasures can negate our precision munitions. In addition, our military is ever more dependent on commercial infrastructure, the security of which is not under military control.

Acquisition

The cycle of systems requirements, research and development, demonstration, procurement, doctrine, training, and deployment in some form is necessary, for at least some major military systems, and it is being streamlined. But, demonstrable advantages often arise from unforeseen technological advances. And in many cases, COTS equipment and services outperform their military counterparts consistently and by large margins. The military must learn how to use inventions, COTS options, and commercial services directly and quickly. In some cases, short circuit of the normal acquisition process, from bench top to field in tens of months, with few reviews, small numbers of systems implemented, and special training, maintenance, and deployment are essential. Otherwise, an asymmetric adversary, with wealth and no constraints, can exploit niche capabilities and do great harm.

Two Edged Sword

As we have discussed in our Workshops, our military can falter by not adopting new methods and technologies, which will be available to our adversaries. On the other hand, these new methods will bring new vulnerabilities. A highly integrated and networked force can be vulnerable to a breach of critical systems, disinformed command, electronic failure, information overload, sensor blindness or deception, destruction of critical nodes, infrastructure attack or failure, and many other nontraditional failure modes.

GLB-5. ECOLOGICAL RISK

The Dilemma of the Commons

Stressed commons are dramatically unstable. The participants are motivated to grab what they can and withdraw. It happened in colonial New England when the common resources, pasturage in this example, were not sufficiently in excess of the community need.

The Earth is feeling human communal stress through the many demands placed by the growing world population and rapidly rising standard of living. The limits of the Earth (and human ingenuity) to sustain us are not well known, and in many respects may not be determinable. We proceed based mainly on faith that, just as the technologies of 1900 could not supply the needs of the population of 2000, we can develop the technologies and find the resources to be able to sustain the populations of the future.

It is well-established that we are changing the Earth in irreversible ways (e.g., reducing biodiversity, altering atmospheric composition and climate) and that we are not in control of these processes. To a high degree we are unaware of the details or directions of the changes we are inducing, and have no assurance that future generations will be able to find the resources and bring more equity to the global standard of living at the levels that we already enjoy. To some, this is the ultimate, and therefore, the most immediate threat scenario.

Contentions

Energy, water, food, land, population growth, biodiversity, and human rights are the principal issues. We have recently gone to war over oil; we need oil to enable our military forces, our industry, our mobility, our security, and the comfort level of our population. We use hydrocarbon energy sources, which are not renewable, at a greater rate than other nations, and we endanger the global climate by doing so. Emerging nations such as China are rapidly increasing their use of fossil fuels, but are still at a per capita level about one-tenth of ours. While wanting and needing to pursue efficiency, accepting limitations on carbon use, and thereby, limitations on the enhancement of their people's well-being in order to protect the environment, is beyond their immediate horizon. It is difficult to condemn these nations too vigorously as long as prudent resource and environment management is also beyond the political grasp of those of us who already have our needs met.

Water is a source of energy, food production, industrial production, transportation, and recreation; in general, it is the blood of life and considered sacred in some places. It flows over and under national boundaries. It is plentiful in a few places, but insufficient over most of the Earth. Current desalination and water transport techn0ologies are too demanding of energy or too costly to provide practical alternatives to available sources except in isolated circumstances. In addition, the preservation of existing water resources comes into conflict with many other human activities, e.g., waste disposal, the green (chemical) revolution in agriculture, and housing development in water resource areas.

Food from the ocean commons is contentious, and is already showing signs of typical "failure of the commons" due to overexploitation. Food production on land requires control of the land, biological specialization of crops that decreases biodiversity, and the use of chemicals that can pollute the local and even distant environment. Eutrophication due to fertilizer runoff in rivers and their outflows into seas and oceans is becoming a very large-scale problem. Food fishers, farmers, and processors are focused on their own products, not on the larger scale effects of their actions.

Land is needed for people to live on and provide for themselves, "lebensraum" as the Germans called it. Other species also need habitat, but they cannot compete with humans.

Human labor and sacrifice by have-not peoples are often substituted for the lack of the other resources discussed above, or for economic reasons. The argument that this does raise up the have-nots by giving them entre' into the global economic system is true, but the transition can be long and harmful.

All of these resources will be jealously sought, fought over, and over-used. These are the derivative threats of unsustainability.

In fact, if sustainable energy sources that do not impact the environment were available, the brunt of the ecological threats would be removed because energy, the most contended resource, can often be used to provide the other contended or strained resources.

Predicting the Future, Even Next Week

The biosphere is always evolving toward equilibrium with human demands. As human activities expand, the remaining life forms must adapt and usually contract. Indeed, the earth systems are being altered by human activities in ways that are not easily discernable, predictable, or controllable.

Better models of the physics of the atmosphere, oceans, and land surface conditions are evolving rapidly and data on these systems are accumulating. Although many natural phenomena (e.g., the weather, volcanoes, earthquakes) are fundamentally chaotic and not predictable beyond very confining limits, broad bounds of prospective consequences of both natural events and human-induced changes can be developed and scenarios developed of the types of conditions that are plausible. While models that encompass the key elements of the spectrum of physical and biological interactions of the biosphere and atmosphere are only starting to emerge, much can be learned about how to enhance societal response to potential threats.

Even as such models become available, however, history teaches that there is always the potential for, even the likelihood of, surprises and unintended consequences from our responses. To assume that society can continue to act in ways that insult the environment, and that society will, with confidence, be able to control or compensate the consequences, is very risky.

The Invisible Hand

Economists believe that if the proper value function can be defined, a market-based system will find its own optimum better than could the wisest planner with the best model: "The free market will provide." Indeed, the global population growth appears to be stabilizing in areas where an adequate standard of living has been achieved; predictions of the asymptotic world population have been steadily decreasing over the past decade. And Julian Simon's prediction that most commodities will decline in price in spite of predicted shortages has continued to prove true. Unfortunately, bio diversity and most environmental needs are not easily or credibly monetized. What is the value of a stable global climate? Of the biodiversity of the Amazon and the marine life of the polar regions? Of consistent weather patterns? Of a constant sea level?

How can we establish international economic and regulatory mechanisms to stabilize environmental parameters and preserve the global environmental commons? How should we weigh responsibility for the global changes versus the rise in the standard of living they have enabled, for economic equity versus reduced environmental threats for the present and for future generations. Experience is teaching us that the invisible hand has its limitations.

Security Over Stewardship

For the US, security, protecting our vital interests, means maintaining our freedom of action, protecting our wealth, and ensuring the availability of the resources on which we depend into the foreseeable future. Yet, this requires more than our proportionate share of the global resources. Were all people to share our levels of wealth and consumption, the threat to the natural world would be greatly increased. And in the near-term, we too would be at risk.

Stewardship of the Earth system and of non-renewable physical and biological resources for our own interests, and for the people of the world, require us to improve the knowledge base for this stewardship, while we also commit some of our wealth and sacrifice some of our consumptive habits for this purpose. Neither of these prerequisites is likely to be available until we are challenged by significant global disruption. This is the nexus of the unsustainability threat.

GLB-6. RISK TO OUR GOVERNMENT

One threat scenario that was discussed extensively in several Workshops was the possible failure of the US as a viable, free nation. This might arise if we were fatally damaged by some horrendous attack on our homeland or some devastating natural disaster focused on one of our great cities, or if our social and economic institutions were seriously degraded. The lack of visionary leaders, or the presence of truly criminal leaders, softness and denial among our well-off people, or the emergence of truly destructive ideological movements are not unique to our time, but are always possible threats, which might incubate in the current rapid changes that technology is bringing. Loss of national confidence, governmental dysfunction, even constitutional failure and the emergence of dictatorship might result.

As will be seen in the following pages, the number of ways in which the homeland can be directly attacked with weapons of terror and mass destruction and with information weapons is increasing. Our openness, civil rights, and guarantees of due process work for the adversary in the short run; adversaries use our social (drugs), political (lobby), legal, cyber, and media (psychological) processes. And our technical preparedness for homeland attacks is not keeping pace with the threat technologies and modalities. In fact, the projected subtlety and complexity of attacks, and the speed with which they might be delivered surpass our ability to model them realistically, and to plan and to implement responses. Deep strikes with clandestine nuclear weapons, or dispersed biological weapons, instantaneous attacks on our commercial and social information systems, as well as high-tech conventional attacks on populations and infrastructure, anonymously executed, are frightening prospects.

In addition, more subtle mechanisms, like extreme inequities of opportunity and wealth, factionalism (social/moral/religious, political/ideological, ethnic), and overuse and deterioration of our environment, can undermine out trust in government.

If the US fails to provide both political (domestic and international law and communality) and technological (prevention, detection, denial, and prompt remediation) responses for these perceived threats, our popular reaction might be fearful and self destructive. Tyrannical regimes of search, personal monitoring, control of movement, information monitoring and control, and limitation on "dangerous" items and activities would atrophy our liberties. We might be more secure, but we would be less free and less viable as a nation. This dilemma calls for significantly better technological defenses in both the real and cyber worlds, and for balance in the protection of personal and common goods.

NUCLEAR, MISSILE, AND SPACE TECHNOLOGY WORKSHOP SUMMARY

On September 21, 2000, a one-day workshop was conducted focused on threats that are enabled by nuclear, missile, and space technology. The participants in this workshop represented the Livermore and Los Alamos National Laboratories, the US Navy, the National Defense University, the intelligence and arms control communities, Senate technical staff, and the defense industry. The following brief summarizes our findings.

PRIORITY THREAT SCENARIOS

- **Nuclear attack on cities (US cities, Tel Aviv, Seoul, Taipei) and high value concentrations (oil fields, refineries, airports) by terrorists, states, revolutionaries, or extortionists**
- **Nuclear deterrence destabilization: major shift in nuclear weapon related capabilities**
- **Tactical nuclear weapons proliferation and use**
- **Nuclear surprise**
- **Loss of control of space: attacks on space assets and from space**
- **Electro-magnetic disruption in the troposphere or magnetosphere**

TECHNOLOGIES WITH THE GREATEST THREAT POTENTIAL

- **Intelligence and espionage technology**
- **Nuclear weapon technology**
- **Anti-submarine warfare: ASW**
- **Space launch technology**
- **Submarine technology**
- **Nuclear armed cruise missiles**
- **Space sensor systems**
- **Information technology**
- **Nuclear material technology**
- **Anti-satellite technology: ASAT**
- **Missile defense countermeasures**
- **National missile defenses**
- **Theater missile defenses**
- **Laser weapons**

UNCERTAINTIES

- **Globalization of nuclear, missile, and space technology?**
- **Intelligence of the globalized world?**

INTRODUCTION

Ironically, advances in technology, which have given the US global military dominance, have obsoleted much of the world's Cold War era systems and motivated emerging nations to nuclear forces, which give them the ability to deter superior conventional forces, formidable weapons, and instant stature in international affairs. Even the US can be deterred by nuclear arsenals much inferior to ours. In addition, the general advance in global technology has decreased the cost to obtain nuclear weapons and their platforms. Computers, isotope enrichment, nuclear materials technology, robotics, precision machining, space launch and intermediate range missiles, cruise missiles, global positioning systems, and satellite imaging are all now commercially available.

The number of potential nuclear proliferators has increased, while international proliferation restraints and transparency have receded due to the waning of cooperative regimes, the emergence of barter economies, and the increasingly dual use of the relevant technologies. Manufacturing agility and virtual distributed industrial complexes discourage identification of proliferant activities.

Global energy and environmental needs will support the continued spread of nuclear energy technology.

Nuclear technology is one of the ships that is rising on the global technological tide.

In addition, there are disturbingly credible scenarios for the future use of nuclear weapons in regional conflicts. If used for defense in a desperate attempt to prevent being overwhelmed in response to a massive attack, a nuclear response might be condoned. In fact, possession of "tactical', that is, short range nuclear weapons for counter-force purposes, might be accepted internationally for national defense. This limited acceptance of tactical nuclear weapons might stimulate their proliferation, particularly in regions of tension, where they are most likely to be used.

Beyond this, modern tactical nuclear weapons can be relatively sophisticated and might imply nuclear expertise on the part of their possessors. This, in turn, increases the probability of further nuclear weapons development, and the potential for their preparation for other uses, such as in space or in other scenarios remote from the "defenders," thus leading to a wide proliferation in number and quality of nuclear weapons. This is the progression that derives from the following scenarios.

PRIORITY THREAT SCENARIOS

NMS-1. NUCLEAR ATTACK ON CITIES AND HIGH VALUE CONCENTRATIONS

The easiest nuclear attack for the minimally technological to prepare and execute would be the detonation of a single or few relatively crude nuclear devices in cities, like New York or Tel Aviv, or in other high concentrations of value, such as, the Silicon Valley. Given relatively little fissile material and a simple inefficient design, or a stolen or procured contraband weapon, hidden in a truck or freight container, such an attack is not difficult to orchestrate and is very difficult to prevent or attribute.

Such an attack could be mounted by a nation of "concern" or terrorist, or even by an apparently "engaged" nation, since attribution would be difficult enough to preclude a confident immediate counter strike. The result would be a very large loss of life and destruction of property, and political and economic chaos, from which the victim would not recover for years. International relations would be in crisis as all sides tried to absorb this disaster, discover responsibility, assess the now extended role of nuclear weapons, and decide how to respond. A response in kind might drive a continuing cycle asymptoting to global scale destruction.

A very frightening scenario would be the nuclear attack of a nuclear reactor with its dispersal of a large amount of very dirty radio nuclides. Lesser variations of this threat might involve the use of radioactive materials dispersed by conventional explosives to contaminate cities or high value facilities. The direct and collateral effects of this attack would be very much less than those of a nuclear detonation; it is likely that more than one device would be needed to achieve a widespread effect.

The probability of a nuclear attack on cities is greatly increased by the virtual impossibility of impenetrable security. However, even nominal effort would represent some deterrent and possibly a significant intelligence and warning improvement. To date responsibility for this protection in the US is not focused and is operating with inadequate technology.

Adversary Weapons and Tactics

- Either procure or construct a few nuclear weapons.
- Model optimum destruction and dispersal.
- Use industrial methods to emplace and detonate it.
- Enhance the damage in either case with psychological warfare.

NMS-2. NUCLEAR DETERRENCE DESTABILIZATION

While the nuclear deterrent situation among major nuclear powers is less tense than during the Cold War, it is more complicated. The number of lesser nuclear powers has increased and might increase further; and the relationships among these potential and new nuclear states are more tense (India, Pakistan; Israel, Syria, Iraq, Iran, and the

Palestinians), and the concerns are more immediate (Kashmir, Palestinian aspirations). Finally, there remain both trigger situations (Taiwan, Korea) and issues of strategic concern (missile defense, submarine forces, MIRVing, weapons control and security, fissile material protection) among the major powers, the elements of which will be dynamic over the coming decades.

During the Cold War, the exchange analysis, targeting, and escalation scenarios were understood by Russia and the US, although hindsight has shown that even in that mathematically simpler case, dramatically different war plans were chosen. Now, the picture is much more complex. There are major, global equations to balance; and there are lesser, local equations, with strong coupling between these sets.

China is a major actor, who has to date chosen a strategy based on smaller numbers of strategic weapons and missiles. Russia is building down strategically, but is maintaining a huge tactical nuclear force; the safeguarding of both of these arsenals is of great concern. The US wishes to protect itself, and possibly others, from attacks in small numbers, with a missile defense system; but this also effects the "balance" with China, whose threat is partially countered by such a defensive capability. The nuclear forces of these major nuclear powers are very asymmetric, with US submarine dependence, Russia and China more land-based and mobile, Russia with nuclear tipped missile defense around Moscow, and with many deeply buried facilities.

These major powers have client states, which are also nuclear armed and in contention. The deterrent assumptions of such as Pakistan (tactical) and India (strategic) are incongruent, which makes their mismatched standoff difficult to stabilize. Israel's immersion in and asymmetry with its antagonists create even greater instabilities. And, finally, Germany and Japan are not armed, but are nuclear capable and might be motivated if they felt threatened and uncertain of their immediate coverage by the US and the NATO/SEATO allies. Nuclear posture and conflict among any of these actors could call the major powers into action.

The fear used to be of a Russian weapon-scientific diaspora, but now many Ukrainian, Georgian, Kazakh, Korean, Iraqi, Iranian, South African, Argentine, and other scientists are both trained and experienced with some aspects of nuclear weapons and materials. At the same time, the US and Allied expertise is dwindling due to the lack of ongoing development programs and the aging of its experienced people.

The growing availability of space launch and space technology increases the likelihood that space will be armed, either with de-orbitable nuclear weapons, or with other weapons that threaten strategic space systems.

The availability of biological, chemical, and cyber weapons further complicates the picture. With even a minimal nuclear deterrent, a state or non-state may be more willing to use these other weapons, because their nuclear capability discourages a punitive response.

Add to this that the intelligence picture is dramatically changed by global transparency, with several satellite systems of high resolution, hyperspectral, imaging sensors; increasingly accurate GPS systems; networks of scientific atmosphere and ocean sensors; a wide open Internet with encryption; industrial, criminal, and terrorist groups with substantial resources, and with intelligence interests and globalized technologies of their own, often willing to sell their information.

The fabric of international nuclear relations is an increasingly complex tapestry.

Adversary Weapons and Tactics

- Develop indigenous nuclear weapon technology and production.
- Obtain fissile materials or enrichment and purification capabilities, such as laser isotope separation.
- Develop portable, tactical, and strategic nuclear weapons.
- Develop nuclear capable bombers.
- Develop tactical delivery systems: rockets, artillery. and ground vehicles.
- Develop long-range rocket and cruise missile systems.
- Obtain missile capable submarines.
- Develop theater and ballistic missile defenses and countermeasures.
- Declare nuclear capabilities that establish deterrence.

NMS-3. TACTICAL NUCLEAR WEAPONS PROLIFERATION AND USE

Tactical nuclear weapons are the great tactical equalizer, in the NATO-Warsaw Pact standoff, and by Russia against the Chinese masses; by the Pakistanis against the superior Indian numbers; by the Israelis; and logically, if not actually so, for other militarily less armed, but technologically advanced nations. If used in self defense, particularly on ones own soil, say Pakistan in fending off an Indian onslaught, or Russia within the Confederation, or in Korea, this use of nuclear weapons might not call down a response by other than the damaged adversary. It would be a limited and domestic affair; but it would establish nuclear weapons in tactical combat and would drive immediate broad proliferation among aspiring nations.

While tactical nuclear weapons are not as strategically threatening as nuclear tipped long range missiles, concern would be greatly amplified by nuclear capability in, say, Iraq or Iran or North Korea or north Africa. In addition to the real threat that these weapons would pose to neighbor states, such weapons would increase the fear that such nations would act aggressively, thereby increasing their perceived ferocity and giving them greater clout in international affairs. The effectiveness of such weapons, the fear that they would generate in neighbors and beyond, and the perceived lack of long-range strategic threat all make tactical weapons more desirable from the point of view of emerging states.

Compact nuclear weapons are technologically difficult to make. It is likely that an advanced nuclear state would have to provide such in the near term. Crude nuclear weapons for tactical use might proliferate first. In either case, these weapons are such a powerful force multiplier, that it is very likely that they will be used eventually and will proliferate, along with more sophisticated nuclear science and technology.

Adversary Weapons and Tactics

- Obtain and declare tactical nuclear weapons.
- Obtain tactical delivery systems: bombers, artillery, rockets, remote vehicles, man portable.
- Use tactical nuclear weapons in defense of the homeland, particularly on ones own soil.
- Develop defenses against theater missiles to counter tactical nuclear retaliation.
- Resist attempts to limit tactical nuclear weapons and relevant technology and materials.
- Declare potential first use if invaded or immediate response if nuclear attacked.
- At first, copy, and then, learn the technology necessary to make tactical nuclear weapons and then variants of these for special situations.

NMS-4. NUCLEAR SURPRISE

Because of enormous effort and motivation on the parts of the leading scientific and technological nations, nuclear weapons achieved their initial optimum realizations in a very short time, within currently perceived applications. However, it is very likely that the evolution of nuclear weapons is not finished, and that future variants and combinations with other technologies are not all yet envisioned.

Particularly as the tide of technology rises around the world, variations on nuclear weapons will become more accessible and, possibly, more imaginative. Penetrators, demolition weapons, radiation weapons, directed radiation weapons, space weapons, EMP weapons, portable and low yield (10 to 100 ton) weapons, weapons that we do not yet imagine because their target is in the future, such as asteroids, space craft, or human habitats for space or deep sea. Platforms will also evolve and will require flexibility of nuclear weapon designs.

Testing, even of exotic concepts, will become less and less needed as computational tools and physics data improve. Materials will be more accessible, handlable, and manipulable. COTS fabrication techniques, agile manufacturing, robotics, and system control electronics will be applicable. State and non-state wealth will be able to support such efforts, as applicable related advanced technology infrastructure emerges.

If, as discussed above, compact nuclear weapons proliferate, their uses and designs will proliferate. These weapons can be relatively sophisticated and the capability to make them would imply the ability to respond to various new applications.

These probabilities argue that nuclear innovation will occur, that sophisticated nations, an ever growing set, will at first accomplish what others have already demonstrated to be doable, and that the new nuclear actors will probably find other uses and configurations. It is prudent for the world leading nations to keep their nuclear expertise fresh and available, even anticipatory, as they try to control the availability of a potentially increasing variety of nuclear weapons.

Adversary Weapons and Tactics

- Obtain scientists and engineers trained in nuclear related technology.
- Obtain relevant design codes and supporting data.
- Obtain materials and machining/handling capability.
- Obtain systems engineering and development capability.
- Develop test capabilities.

NMS-5. LOSS OF CONTROL OF SPACE

The US Air Force plans to become the US Aerospace Force, integrating air and space assets and operations, and providing the US with continued air and space dominance. This plan includes a mix of military assets and commercial capabilities, the latter to achieve reduced cost and the rapid performance improvement afforded by commercial developments. It would appear that currently no nation or faction can approach the US space program in support of military operations.

At the same time the US AF will depend to a greater extent on commercial space launch capabilities, capabilities that other second and third world countries already have, and that third other world countries are developing and will have access to within the next two decades. In addition, capabilities for communication, navigation, environment and weather monitoring, and reconnaissance, originally the sole property of the military, are now civilian/commercially available, are rapidly improving in performance, and are dominating space in numbers of space craft. The population of US space assets will soon be immersed in a greater population of international space assets from all quarters and persuasions. Space will resemble a global port city in diversity.

Again, it is improbable that any entity will soon threaten the US massively in space or defeat the US space control capabilities, but there will be opportunities for asymmetric advantage by adversaries, placing intelligence assets in space, tampering with both commercial and military systems, attacking isolated assets, possibly in connection with ground and sea operations, and launching ground, sea, and air attacks from space.

As the population of space systems grows, it will be more difficult to know what is in space and to surveil space activities. It will be difficult to attribute attacks in space and from space. Much of the US space control force is still only a plan and could be challenged before it is complete or at any time outside the envelope of its capabilities. Space still resembles the Old West in that it is a sparse, minimally patrolled, orderless place, with few rules and no police. The global onslaught into this vacuum will be an opportunity for some outlaws of concern

Adversary Weapons and Tactics

- Use commercial collaborations to gain satellite and space vehicle technology.
- Use international commercial surveillance, communication, and navigation services for intelligence and military purposes.
- Preplace space weapons in the guise of commercial space assets.
- Use scientific collaborations to gain intelligence, technology, and data.

NMS-6. MASSIVE ELECTROMAGNETIC DISRUPTION (See GEO-9.)

The EMP threat is significant both regionally and strategically. As one version of a defensive tactical strike discussed above, EMP used in a regional conflict is less lethal than a direct counter force strike, thus more condonable, while it could be extremely effective militarily, making this a relatively high probability use. A strategic use requires significant launch and nuclear weapon sophistication, an unlikely third world threat for the foreseeable future. However, given the sophistication, a large nuclear device might be launched over the central US to an altitude of 400km to 500km and detonated, emitting a very large EMP which could "burn down" much of the US electronic and electrical infrastructure. A large fraction of the US space assets might also be destroyed. The ionosphere could remain radio hot for many months.

The direct damage could be in the trillion dollar range, since commercial systems are not hardened. The loss of future business and thereby of projected market value would exceed this and would be recovered slowly, because of the lack of the destroyed infrastructure and the lack of confidence to reinvest with any assurance that a repeat attack could be prevented. Such an attack would make us both strategically and tactically vulnerable to a follow-on all-out attack.

Such an EMP attack could be launched from the near ocean, and might have little warning and no direct attribution. Our vulnerability and inability to respond would be nationally depressing, even without any follow-on attack.

Adversary Weapons and Tactics

- Develop "portable" launch capability, say, floatable sea launch rockets.

- Procure high yield, space capable nuclear weapons designed for maximum electromagnetic pulse and ionizing radiation.
- Harden or plan the event to minimize harm to perpetrator's electronic systems.

NUCLEAR, MISSILE, AND SPACE TECHNOLOGIES WITH THE GREATEST THREAT POTENTIAL

1. **Intelligence and Espionage Technology.** The ability to penetrate secret information systems and data bases, obtain secret computer codes, use human and technical intelligence methods, and assemble complete sets of nuclear weapon system and platform designs; knowledge of our and others capabilities, intentions, and operations; in general, the ability to obtain and understand nuclear weapon system information.

2. **Nuclear Weapon Technology.** The ability to design and produce, from the basis of nuclear, radiation, materials, and hydrodynamic physics to the engineering implementation of systems, nuclear devices and weapons, either crude, large, and cumbersome , or sophisticated, compact, more easily concealable and ultimately space qualified and hardened; ability to tailor nuclear devices for specific blast and radiation effects, such as EMP.

3. **Anti-Submarine Warfare: ASW.** The ability to detect, track, target, and destroy submarines, including global sonar, radar, and hyperspectral sensor systems, sophisticated search and detect analysis tools, stealthy submarine tracking and attack systems; miniature submarine sensor/tracker/pursuers; ELF radio jamming.

4. **Space Launch Technology**. For delivery of nuclear weapons, indigenous intercontinental ballistic missile capability with adequate load capacity and relatively crude guidance (GPS); for placement of weapons in space, either indigenous capability or simply the ability to conceal weapons in apparently non weapon guise and then use commercial space launch services.

5. **Submarine Technology.** Quiet, fast, long submersion, torpedo, rocket, or cruise missile capable submarines, either nuclear or diesel powered, such as the Kilo-class diesel subs or better; coastal and river capable submarines.

6. **Nuclear Capable Cruise Missiles.** Cruise missiles capable of carrying the load of the nuclear weapons available to this adversary to a range of at least hundreds of kilometers with accurate navigation and

terminal targeting and guidance or tracking; with stealth and counter-countermeasures.

7. **Space Sensor Systems.** Sensors able to see hyperspectrally from radar to the UV with high resolution, moving target discrimination, and real-time coverage, such that intelligence can be gathered and operations can be monitored and controlled; special sensor and analysis tools for finding concealed targets and submarines.

8. **Information Technology.** The ability to perform C4ISR activities for the delivery and control of nuclear weapons, and coordinate agents and forces in support of these activities; ability to find and attack adversaries defensive information systems; ability to confuse or disable by information operations adversaries' communication, navigation, or surveillance systems.

9. **Nuclear Material Technology.** At least the ability to perform manufacturing operations with fissile, exotic metal, and explosive materials, and additionally, the ability to enrich (AVLIS), chemically process, and form fissile materials, including automated and remote processing, forming, handling, assembly, and storage with relatively safety and adequate quality.

10. **Anti-Satellite Technology: ASAT.** The ability to place in space satellites and objects capable of finding and destroying or disabling satellites, stealthfully and unattributably; micro-satellite technology; directed energy weapons; EMP; high power microwave beams.

11. **Missile Defense Countermeasures.** The ability to prevent interception and warhead disablement of ballistic and cruise missiles by stealth, electronic countermeasures, decoys, or other means, such as, terrain following or undersea approach.

12. **National Missile Defenses.** Boost or midcourse capability to detect, recognize, intercept, and destroy intercontinental ballistic missiles, overcoming their countermeasures and disabling their warheads, operating from land, sea, air, or space.

13. **Theater Missile Defenses.** The ability to detect, intercept, and destroy, disabling their warheads, short and intermediate range ballistic missiles.

14. **Laser Weapons.** Directed energy weapons capable of anti-satellite, anti-aircraft, anti-sensor, or even anti-missile energy, power, and pointing; ground, air, or space based; possibly for point defense.

UNCERTAINTIES

1. Globalization.

Will the balance of global technology diffusion and wealth creation tip toward peace and cooperation or toward the use of these new capabilities and capital resources for aggressive, domineering, even warfighting capabilities, particularly nuclear weapons, which destabilize international relations?

2. Increased Intelligence.

As globalization projects the US to the far corners of the earth, will we be culturally adept, understand the local customs and motivations, appropriately use business, government, and social contacts to learn, to increase our world awareness, to give us better early warning of troubles, instabilities, and dormant disputes, of causes of war that are not apparent from our context, but are, never the less, potent and potentially harmful to us?

MILITARY TECHNOLOGY WORKSHOP SUMMARY

On July 25, 2000, a one-day workshop focused on threats that are enabled by military technology was conducted. The participants in this workshop represented the Livermore, Sandia, and Oak Ridge National Laboratories, the US Army, Navy, and Air Force, DARPA, the intelligence community, the defense industry, and university research centers. The following brief summarizes the workshop findings.

PRIORITY THREAT SCENARIOS

- **C4ISR failure by the military**
- **Urban warfare catastrophe**
- **Tapestry attack on the US homeland**
- **Focused attack; deep strike in CONUS**
- **Retreat to CONUS and inability to project global power**
- **Loss of air strike capability in opening phase of conflict**
- **Failure to dominate a dedicated modern asymmetric adversary**

TECHNOLOGIES WITH THE GREATEST THREAT POTENTIAL

- **Information technology for military C4ISR and for tapestry activities**
- **Infrared imaging sensor focal-plane arrays (IRFPA)**
- **Bio weapon platforms**
- **UAVs and robots**
- **Covert nuclear weapons**
- **COTS systems for urban warfare**
- **Smart mines**
- **Man portable missiles**
- **Cruise missiles: stealthy and intercontinental**
- **COTS C4ISR**
- **Quiet diesel submarines**
- **Precision and smartness**
- **Chemical weapons**
- **Simulation for planning and training**
- **Ubiquitous sensors**
- **Blind spots, deception, and concealment**
- **Directed energy**
- **Modern explosives**
- **Stick and slick substances**

INTRODUCTION

The US can dominate adversaries in symmetric engagements; we have the asymmetric advantage in a "fair fight.," that is, in large scale force on force warfare. But, we are also asymmetrically vulnerable, having large concentrations of people and wealth, and globally distributed interests that are difficult to defend, particularly against a suicidal attacker. We try to respect the law, national sovereignty, people's natural and civil rights, property, and the environment, while asymmetric adversaries are not so constrained, and in fact use these foibles of ours for their own purposes.

The African embassy bombings killed a dozen US citizens, while killing 200 Africans and wounding 4,000. The perpetrators were from six nations (apparently including the US) which did not condone or know about their actions. It is likely that the US will have to deal with this kind of "asymmetric warfare'" in the future.

However, as badly as we may be hurt by terrorism, we will not be defeated by asymmetric adversaries. And as we develop specialized counter forces and adopt "virtuous" versions of their techniques, their advantage and effectiveness might lessen.

Perhaps the greater fear is that our asymmetric military advantage will diminish, as improved IR and radar systems diminish the effectiveness of our stealth and our countermeasures, as improved range, speed, and stealth of anti-aircraft and anti-ship missiles push our support systems back from the theater, and as satellite systems improve the adversaries intelligence. In addition, their use of C4ISR for their own purposes and to defeat our C4ISR systems might shift the information technology imbalance away from us. In general, we can expect the battlefield to become more transparent for them and more opaque and dangerous for us.

The overall effects of adversaries advanced technologies will be to increase the effectiveness and reach of their forces. It is probable that we will experience more casualties, even well behind the "front". The adversaries will be more difficult to suppress, with stealth, expendable and intermittent systems, and undergound and camouflaged facilities. Both air and sea operations will be increasingly difficult, due to the stealth and reach of their missiles.

Our defense forces will be called upon to protect our global interests, our homeland cities, and our infrastructure, and to be prepared to deal with biological and chemical attacks. This will focus more of our defense resources on our homeland.

The bottom line is that the US will be less likely to intervene outside of the US, and will be more wary in protecting our home.

PRIORITY THREAT SCENARIOS

MIL-1. C4ISR FAILURE BY THE MILITARY (Same as IT-3.)

Vision 2020 is based on information superiority and the pervasive use of information technology in all US military systems and operations. While this is necessary to maintain dominance, it introduces new vulnerabilities and failure modes, many of which are not foreseeable. On the one hand, it is feared that the military culture and acquisition process of our multi-purpose forces will prevent continuous and timely adaptation and implementation of the most effective technology, thus losing advantage to smaller, more flexible, specialized adversaries. On the other hand, it is feared that complete dependence on highly integrated information systems will create systemic vulnerabilities and failure modes. Every new capability introduces a new set of doctrinal, organizational, and tactical problems.

Some of the former concerns are that:

• Service traditions and doctrines have proven effectiveness, but cause stagnation, protect the status quo, and impede dynamic adaptation;

• the acquisition process, after many attempts to improve it, still prevents technological responsiveness to COTS innovations; is too platform, hardware, and process oriented, and bureaucratic; is bound to legacy systems and standards; and fails to recognize the shortness of information technology development time scales and system lifetimes;

• joint-command C4I is culturally extremely difficult, implying a more distributed command structure within Service units and much more cross-Service integration, dependence, and trust, all requiring revolutionary organizational and command responsibility changes;

• joint-command C4I is technically extremely difficult because most of the Services' systems have evolved independently in both hardware and software, and are now integrable only with efforts which can exceed the value of the systems; one workshop participant commented, "For the future, while interoperability might be an acceptable requirement, it represents the failure of true system integration; the guiding principle for information integration within the commander's priorities should be *from each sensor capability to each decider need.*"

On the other hand,

• too much information can cause saturation and warrior/decider failure.

• highly efficient systems operate near the edge of performance, are less tolerant of saturation or delay, are less redundant and more prone to single point failures, and are less able to cope with out of scope situations; standardization enables integration, but diminishes hybrid vigor and redundancy; digital systems are flexible, but analog backups are not being provided; there are valid questions as to whether the initial systems of the future will be more robust or more brittle.

• highly integrated systems imply potential system-wide access for the intruder and far-reaching consequences of subsystem failures; wireless systems become unintended sensors and unit locators for adversary's reconnaissance and intelligence.

• commitment to highly evolved systems forces command decisions to be made within the performance envelop of these systems, limiting military and political flexibility; will dependence on defined system capabilities and the fear to commit people, who are very flexible systems, to dangerous situations limit our ability to project and credibly deter?

Adversary Weapons and Tactics

• Globalization means that many of the military system elements are accessible to adversaries' influence such that they can both frustrate acquisition and take advantage of known vulnerabilities, and imbed malfunctions, hostile agents, and system self-destructive effects; also, adversaries will have the same technological opportunities that we have.

• Integration of US forces and systems with those of our allies and international organization collaborators affords other opportunities for far reaching intrusion, operational denial, and misdirection.

• Reliance on COTS and open standards and protocols in a complex networked system of systems is inherently vulnerable to attack. While the defender must provide robust defense of the entire system, while enabling external access, the attacker gets to choose the "weakest link," of which some examples are as follows:

• Use accessible sources to embed Trojan horses; violate the still used concept of trusted software.

• Exploit the vulnerability of wholly integrated sensor/targeting/control systems; attack sensors, information nodes, logistic nodes, control nodes; jam uplinks to satellites and aircraft.

• Attack the information system: corrupt message synchronization, protocols, and encryption; cause system restarts; saturate lines with number and size of transmissions; modify routing; cause desynchronizing transmission delays.

• Attack control and communication system infrastructures: power, distribution, terminals, switches, repeaters, buffers, and storage.

• Attack on-board processors with code disruptions, electrical noise, and EMP.

• Corrupt situation awareness with information denial and disinformation; inject false information and bad data to mislead, confuse, and subvert trust; undermine the credibility of command, a single-point failure node.

• Corrupt system embedded and supplier provided training software.

- Frustrate cryptography to get the operator to turn it off and then intercept; sniff for information signal leaks; perform message traffic analysis.
- Exploit built-in telecommunication maintenance features, such as supplier provided remote access and diagnosis features not used in the specific application.
- Use LEO, broad-area, nuclear EMP or local, terrestrial, explosively or electrically driven EMP.

Possible Response

Simulation of new technologies, acquisition and support methods, force structures, and tactics will provide some basis for implementation decisions and vulnerability avaoidance. Simulation is also a tool for persuasion, planning, and training, and a method for red-team vulnerability analyses. These analyses can help to ensure the necessary system features (robustness, redundancy, openness, modularity and designed ease of upgrade), and could provide demonstrations of the value of unconventional, innovative tactics and technologies in combat and information warfare, and of the effectiveness of defensive tactics against conventional and asymmetric attack.

MIL-2. URBAN WARFARE CATASTROPHE

Guerilla warfare in cities using both future conventional military and COTS technology is a challenge for the US military and civilian authorities. Preserving the high-value civilian environment and avoiding civilian casualties will be very difficult when devastation and death are the objectives of an asymmetric adversary. Military weapons for containing and destroying similarly equipped enemies are not designed for low collateral damage, as is desirable in cities or other high-value environments. Most combat aircraft are obviously not useful in the city. Battlefield ISR technologies are much less effective in a city; military sensors are not designed for urban environment where a sea of humanity and a forest of buildings hide hostile activities. Smartness and precision are essential for urban war fighting and defense, but these methods are also becoming globally available. Urban situation diagnostics and defensive responses for large-scale operations are not well developed; our cities, most cities are not designed for security and defense on a military scale or against terrorist hostility.

On the other hand, cities are ideal for terrorism and asymmetric tactics. There is an extreme density of value, no hardening or defensive structures, infinite places to hide and conceal weapons, many people at risk and among whom to blend, a good environment for automated systems, energy sources, and communications, and high visibility for dramatic effects and political impact.

Adversary Weapons and Tactics

There are many options for the adversary:

- Nuclear, biological, and chemical weapons.
- Infrastructure ruination: electric power and water systems are accessible; liquid and gaseous fuels are both accessible and useful as weapons; communications are both vulnerable and useful to the attacker.
- Destruction of buildings, terminals, and other high population facilities using conventional explosives strategically placed or fuel air explosives.
- Traps and ambush: booby traps and lethal decoys, traps in traps (second bomb), and coordinated remote controlled devices and ambushes are ideal for the closed, densely populated spaces in cities.
- UAVs and robotic devices: the city is an ideal environment for automated systems that prefer pavement and orderly clear space for their operations: ground and air micro UAVs and mobile robots for intelligence and attack, and mobile smart and disguised urban mines.
- COTS information systems: C4I on the telephone and the Internet, encrypted or carried on low-probability-of-intrusion, low-probability-of-detection dedicated systems, unmanned sensors, and 3D maps updated in real-time of buildings, transportation, and other infrastructure.
- Anti-IT: EMP and jamming (with expendable jammers and pulsers) of telecommunications, computers, and GPS; and microwave chip burners and silicon eating bacteria and chemicals.
- Panic and confusion causing information: disinformation, data corruption and destruction, service denial, and false alarms.
- Paramilitary paraphernalia: body armor, personal communications, and remote personnel identification.
- Military systems: night and thermal vision and jammers (bloomers), bullet tracking and fire control, and anti-personnel lasers.
- Sub-lethal infirming weapons to burden the medical infrastructure; incapacitants; and slip, stick, and smell substances.
- Fast underground tunneling equipment.

MIL-3. TAPESTRY ATTACK ON THE US HOMELAND

Tapestry attacks are many faceted (military targets, civilian infrastructure, commercial and financial assets, population and value concentrations), multiply phased (cascaded to maximize confusion and damage, to frustrate response, and to dispirit the victim) attacks across a wide area, even the whole country.

The evolving ability of any group to use the Internet and private networking systems to access public and private systems, to organize forces and affinity groups, and to plan and execute hostile operations is unprecedented. On the one hand, the scope and impact of an attack based on these capabilities is limited only by imagination. On the other, to conceal and execute such a complex operation is not simple, as is evidenced by the failure of such as the Aum Shin Rykyo attack and the absence of such attacks in general.

Denial of service and cyber pathology attacks long anticipated and now numerous, the year-2000's extreme stress on the air transportation system during the summer storms and strikes, daily class 1, 2, and 3 electrical utility crises, the drought-enabled fires in the western US, the arrival of lethal new pests (glassy-winged sharp shooter) and diseases (West Nile virus) in US fields and cities, and the intentional, extreme freedom and anonymity of the cyber world, are all potential elements of a coordinated, distributed attack on a stressed US homeland. Such an attack might be initiated ambiguously, appearing to be an unusual coincidence of negative events, then escalated to full impact just when civilian systems reach their stress limits, all without attribution or even awareness that the events are intentional.

Consequences might be economic panic, actual physical devastation and loss of life, and loss of confidence in civil authorities and the federal government. This attack might be the preemptive precursor to military action here or elsewhere or an attempt to lessen our resolve and shrink our influence.

It should be noted that some of the Workshop participants felt that an attack of this complexity would be very difficult to coordinate, and even more difficult hide. Consequently, it was thought that such an attack would not be successful unless it was confined to a few focussed, devastating actions, for example, like the coordinated embassy bombings in Africa.

Adversary Weapons and Tactics

- Anonymity and globalization: Use the anonymity, difficult traceability, and indecipherability of the cyber world to hide actions and prevent attribution; use COTS materiel from around the world to impede attribution.
- Preplacement: preposition cyber attacks, explosives, and bio and chemical bombs.
- Information: disrupt telecommunication (C4ISR and civilian) and broadcasting.
- Disinformation: create ambiguity, prevent detection before effect, prevent verification, deny information, and instill uncertainty and then panic.
- Physical infrastructure: blowup buildings, disrupt the power grid, destroy pipe lines and refineries, attack fuel tankers in port, disrupt and contaminate water supplies.
- Agriculture and food: use commercial and general aviation to distribute agro pests and pathogens, corrupt food storage, contaminate irrigation, and propagate malignant crop mutants.
- Agents: use UAVs, robots, MEMS, and microsensors for intelligence and precision attacks.
- Explosives: fuel-air, volumetric bombs, and plastique for concentrated targets.

- Response centers: attack response teams and facilities, hospitals, and centers of response authority.

MIL-4. FOCUSED ATTACK; DEEP STRIKE IN CONUS

In contrast to the distributed tapestry attack described above, focused attacks on targets of extremely high value are efficient, low cost, and require less organization, such as attacks on concentrations of government leadership, dense concentrations of people, city centers, nuclear reactors, huge buildings, information control centers, warships in port (USS Cole), large aircraft, trains, and commercial ships. Many of these targets are relatively vulnerable and undefended, particularly against smart, long-range, precision weapons. The US is open and accessible with thousands of miles of coastline. We have atrophied air defense, limited theater missile defense, none in-place at home, and no ICBM defense.

Adversary Weapons and Tactics

- Missiles: ManPAD and (shoulder fired) and SA-10C with IR and EO sensors; long-range (and short-range) cruise missiles; new Mach-10, long-range, hypersonic missiles; ICBMs and IRBMs, although these are clearly traceable and therefore probably deterrable.
- Explosives: fuel -air and 10-ton truck bombs; shaped charges.
- COTS ISR: French SPOT satellite imagery; mapping services.
- COTS navigation: GPS.
- Commercial air and sea craft: can carry much larger explosives and act unsuspectedly; can distribute bio weapons without leaving normal charted lanes.
- Nuclear, biological, and chemical weapons.

MIL-5. RETREAT TO CONUS AND INABILITY TO PROJECT GLOBAL POWER

The US is leaving many of its historic forward bases. Previous allies are becoming reluctant to provide temporary basing or even passage across their territory. Aircraft carriers may become too threatened or actually too vulnerable to risk close in to hostile areas. The US will depend on deep (intercontinental) strike capabilities, large fast air transports, and expeditionary forces. Unfortunately, these capabilities are evolving slowly and may not keep pace with the extent of our withdrawal. Political forces may push us outside of our systems' performance envelope. Does this resemble the retreatism of the 1930s, an increase in strategic threat for our allies, and a loss of global influence?

Adversary Weapons and Tactics

- Discourage Allies from supporting the US with protest and terrorism.
- Negate carrier task force:

  Rising mines,

Small diesel submarines,
Submarine platforms with AIP (air independent propulsion),
Low-observable cruise missiles,
Low-observable torpedoes - wake homing,
Super-cavitating high speed torpedoes,
High speed explosive- and missile-equipped boats.

- Anti-submarine warfare:

Computer tracks,
Active sonabuoys,
Brown-water (littoral) sonabuoys.

- Attack (contaminate) transportation nodes and fuel supplies.
- Real-time surveillance from space.
- Negate US stealth: multi-static radar, infrared imaging, radio triangulation.

MIL-6. LOSS OF AIR STRIKE CAPABILITY IN OPENING PHASE OF CONFLICT

Technologies are becoming available which threaten our ability to take air control and then contain and damage adversaries in the opening phase and continuance of a conflict. Long-range anti-aircraft missiles, which force stand-off of AWACS such that targets cannot be seen or identified or targeted before they can hide, also threaten high-altitude bombers. Infrared-imaging focal plane arrays (IRFPAs) threaten aircraft countermeasures. Multi-static and mobile or expendable radars can counter stealth and negate the effectiveness of anti-radar missiles. These systems and tactics would hold at risk our bomber, reconnaissance, and fighter/attack aircraft, without the need of competing aircraft. Fixed targets can be attacked using long range precision guided munitions (GPS/INS guided). Computer, network, and electronic systems are threatened by EMP/HPM weapon technology. While the adversary might have better field visibility, we might be electronically blinded.

Adversary Weapons and Tactics

- Longer-range IRFPA guided surface-to-air or air-to-air missiles: Russian SA-10C and possible dual mode guided (IRFPA/radar) follow-ons:

-Too great reconnaissance stand off.
- Inability to find targets due to standoff and concealment.
- Too great weapon platform standoff.

- Advanced IR systems: IRFPA, silent radar, IR signatures, IR targeting and homing.
- CLO (counter low observable: e.g., Czech system) radars, which increase range and lengthen attacker time lines; integrated multi-spectral sensors, detection of holes (shadows) in sky background noise.
- Advanced radar computers: processing power increased radar effectiveness.

- Radar protection: shoot at aircraft and move installation: "shoot and scoot;" radar decoys; location disinformation/deception.
- Cheap expendable radars, electromagnetic spectrum control, false signals, and jamming.

MIL-7. DEDICATED MODERN ASYMMETRIC ADVERSARY

A stateless adversary with adequate resources, although no match for the US military, could cause us a great deal of trouble and perhaps extort their political wishes. Such an enemy might resort to urban warfare, tapestry or focused attacks, information warfare, biological devastation, even attacks on our embassies (Africa) and military forces (Service quarters in Saudi Arabia, USS Cole), or any of a wide range of other unconventional tactics. These might be in league with rogue states or terrorists (bin Ladin), or might be a resourced "affinity" group. They would probably have no home to lose and not be concerned about expending their own lives, undeterrable, with nothing to lose. For these people, everything is a weapon and anyone might be their target. They are difficult to predict, to find, and to defeat.

Adversary Weapons and Tactics

- Battle space chosen by adversary: city, mountains, jungle.
- Anonymity amid openness; ghost attacker.
- Close-in, immersion attack prevents systems mode response; air and military power are ineffective, lacking usual targets.
- Complex defender logistics: tenuous distributed adversary.
- Select high-effect technology; systems of systems are not needed.
- Information operations on commercial telecommunication infrastructure, Internet for C4I, access to public information.

MILITARY TECHNOLOGIES WITH THE GREATEST THREAT POTENTIAL

1. Information technology for military C4ISR and for tapestry activities. This extremely broad and growing array of technologies will be at the top of every threat list. Here it refers to dominance, opportunism, subversion, and defense in military C4ISR applications and in asymmetric warfare.

2. Infrared Imaging Sensor Focal-Plane Arrays (IRFPA). The emergence of infrared focal plane arrays enables target/decoy discrimination and negates current IR countermeasures widely used in A/C defense against IR guided surface-to-air and air-to-air missiles. The IRFPA technology also supports much improved long range target acquisition and tracking in a silent, not-jammable mode. In addition, wide field of view infrared optics are greatly expanding the engagement envelope of short range dog-fighting combat. The development of conformal optics for IR missile domes significantly reduces drag, allowing much increased speed and range on IR guided missiles. This combination of technologies is very threatening to our aircraft. Importantly, the proliferation of low cost IRFPA technology in ground combat systems will deny us our current great advantage in night combat; no longer the boast, "we own the night". In addition, IR search and track systems (IRST) for aircraft target acquisition and for ground-based anti aircraft installations avoid aircraft radar threat warning and electronic countermeasure systems.

3. Bio Weapons Platforms. Weaponization and delivery systems for bio weapons greatly increase this threat, the active ingredients of which are extremely compact, more and more available, and evolving in subtlety and effectiveness.

4. UAVs and Robots. The most threatening use of these devices is as weapons platforms which can stealthfully and anonymously attack on the ground, through the air, and from or in the water. In addition, they can perform ISR and fire control surreptitiously and leave no trace. These systems are currently in a phase of rapid and widespread development and will increase in effectiveness as advanced sensor and information technologies are integrated into them.

5. Covert Nuclear Weapons. The nuclear technology is not new, and is the most devastating of all covert weapons. Nuclear weapons are a great military force multiplier and afford greater flexibility in the use of all military weapons by deterring response. But, while bio weapons are potentially as lethal and are more accessible, they cannot match the immediate and total devastation of nuclear weapons.

6. COTS Systems For Urban Warfare. The potential for readily available commercial services and equipment to assist in the organization and execution of urban and tapestry warfare is clear, although these activities would be detectable and are as yet infrequent. Counter COTS technology for the adversary, such as, interception, deciphering, cyber pathogens, EMP, and jammers, are also increasingly available.

7. Smart Mines. As we grow more dependent on the Navy for force projection, and as mines become smarter and faster with more lethal warheads, this threat will increase.

8. Man Portable Air Defense (ManPAD) Weapons. ManPADs enable point attack anywhere on commercial air and other forms of transport, as well as on buildings and for assassination.

9. Cruise Missiles: Stealthy and Intercontinental. Cruise missiles will increase in range, payload, speed, stealth, and versatility, and will become more available. Stealthy diesel submarines are currently available commercially, equipped with cruise missiles. These are one of the principal threats for deep strikes against the US and against the fleet.

10. COTS C4ISR. Open sources account for much intelligence; and as the data bases, news services, publications, and even detailed technology proliferates on the Web, the value of open source intelligence will increase. The Internet can be the means for organization, planning, and execution. In addition, satellite imagery and GPS with very high precision offer both targeting and guidance to any adversary at virtually zero cost.

11. Quiet Diesel Submarines. Kilo class submarines are commercially available equipped with cruise missiles, torpedoes, and mine and sonabuoy laying capabilities, for sea warfare or coastal or deep strike attacks.

13. Precision and Smartness. To date, the US and coordinated allies have been the only belligerents to use smart, precision munitions effectively. But these technologies are rapidly becoming widely available and will eventually become the weapons of choice for terrorists and other asymmetric combatants.

14. Chemical Weapons. As part of a tapestry attack of many elements or an attack on a city or inclosed facility, chemical weapons are extremely effective and terrifying. The Bhopal incident demonstrates the stealth and lethality of a gas attack. Terrorists can use indigenous chemical inventories, such as chlorine stored for water purification.

15. Simulation for Planning and Training. This technology, which has given the US a major advantage in training personnel for all phases of combat, is commercializing both as computer games and as serious training simulators for many professions and military operations. Combatants will be able to rehearse their actions at all scales before revealing their intentions.

16. Ubiquitous Sensors. Micro-miniaturization will increase both the stealth and versatility of remote sensor/actuator devices. Today, advertisements describe commercial clothing, which contains Internet and audio/visual devices. Being "wired" might soon mean a camera and transmitter in a button or contact lens, available at Radio Shack.

17. Blind Spots, Deception, and Concealment. We have not yet solved the problem of surreptitiously, continuously, hyperspectrally surveilling at high resolution any location on earth. By timing to avoid satellite passes, camouflage, functional duplicity, and use of natural blinds (clouds, foliage, terrain), adversaries still operate without our knowledge or ability to interdict. They can fly below our radar in some cases. In addition, more and more facilities have been moved underground, where they cannot be seen or attacked. Such facilities offer inexpensive refuge for asymmetric adversaries, as well as for national forces, and have been employed successfully against us in the past.

18. Directed Energy. As information systems and space assets increase in military importance, directed energy, which does not have the extensive commercial/military dual use of much military technology, will reemerge for EMP, anti-sensors, anti-platform, and anti-personnel uses. This technology has been slow to evolve, but has made steady progress and will find many belligerent applications and much wider availability in the near term. Look for blinder/dazzler laser weapons to emerge first for use against pilots and against IR guided missiles.

19. Modern Explosives. As the USS Cole incident demonstrates, knowledge of explosive's configuration, and material enhancements can greatly increase the destructive effect of advanced conventional explosives.

20. Stick and Slick Substances. Particularly if contaminated with hazardous materials, man or truck portable and dispensable mists and fluids can destroy fine equipment, cause great confusion, and frustrate defensive response or any coordinated activity, particularly in an urban or other high value setting. In addition, less sophisticated variants will eventually be used by protestors and terrorists to shut down critical response facilities without incurring the onus of outright destruction.

INFORMATION TECHNOLOGY
WORKSHOP SUMMARY

On July 26, 2000, a one-day workshop focused on threats that are enabled by information technology was conducted. The participants in this workshop represented the Livermore, Sandia, and Oak Ridge National Laboratories, the US Army, Navy, and Air Force, DARPA, and the intelligence community. The following brief summarizes our findings.

PRIORITY THREAT SCENARIOS

- **Disinformation**
- **Financial destabilization**
- **C4ISR failure by the Military**
- **Critical infrastructure attack**
- **Failure of cyber policy and law**
- **Globalization era intelligence and response failure**
- **Losing to superior cognitive computing**
- **Empowerment of adversary groups**

TECHNOLOGIES WITH THE GREATEST THREAT POTENTIAL

- **Tapestry attack simulation model**
- **Computer system attack technology**
- **Tactical EMP**
- **SIGINT collection technology**
- **ASAT against sensor, navigation, and communication systems**
- **Cyber anonymity, deception, and concealment**
- **Jamming**
- **Reconnaissance imagery**
- **Micro power sources for micro devices**
- **Encryption**
- **Locators for wireless devices**
- **Cognitive computing**
- **Covert communication hardware**

UNCERTAINTIES

- **Degree of military success with information technology?**
- **Micropower technology?**

INTRODUCTION

Before introducing the specific threat scenarios, some general observations on the cyber revolution are in order. First, the rate of "time" in the cyber world is 2 to 4 times faster than historic time; it is estimated that cyber innovation and technology improvement achieve in 3 months what other technologies attain in a year. On this basis, the 15 to 20 year horizon for this study is the equivalent of more than 60 years in cyber time. The result, according to one knowledgeable participant, is that "whatever you can imagine for information technology will happen in this time frame."

Second, information and information technology are inherently global. Networks reach all parts of the globe instantaneously regardless of natural and man-defined boundaries, language, or status.

Third, each information capability also defines a vulnerability. Information is also intelligence; interaction can easily be conflict; access, intrusion; exchange, robbery; persuasion, propaganda; and so on.

Finally, cyber crime is still relatively unconstrained and retribution free. The perpetrators act anonymously, from unkown sites, and, even when caught, are treated as white collar criminals, the loss of money or information being much less onerous than physical harm.

Currently, the information defenders (individuals, businesses, and the national security entities) are not well coordinated for diagnosing attack, defending, or counter attacking. While the defense community is evolving toward better integration and defense, and the banking/financial community is reasonably secure, hackers, individuals, academics, and customer interaction businesses are by choice less constrained or protected by security mechanisms and procedures. The consumer market values freedom and convenience, distributes the costs of attacker damage, and abhors the complexity of protection. As a result the Internet remains relatively unprotected, slow to diagnose malicious acts, and slower still to counter them or find and prosecute the malefactors, in spite of the year 2000's many and overall costly attacks.

Nations are developing the capabilities for more comprehensive and sophisticated information system attacks; undoubtedly, nonnational groups are doing the same on smaller scales. The purposes range from surreptitious and intrusive intelligence gathering, to subtle bleeding of adversary's wealth and economic efficiency, to preemptive strikes in the opening phases of conflict and multi-facetted tapestry attacks during war, and to disruption of key tactical and strategic military operations. With national resources behind them, these methods could become more stealthy and effective, outpacing the development of defenses, which are being only weakly exercised in the absence of international information warfare. Gradually, these information weapons and criminal methods are becoming public and accessible to a wider range of disruptors.

Individuals, businesses, and national entities should link defense efforts, sharing data and analyses of information attacks. Commercial reticence creates asymmetry favoring the attacker, whose hacker technology is widely shared, while sharing among the defender communities of their attack experience, perceived vulnerabilities, and defensive measures is constrained by the desire for commercial advantage and by fear of the vulnerabilities created by revealing their weaknesses. Similarly, exchange between the open and national security communities is not yet productive. Clearly, the next decade will see major information operation events and the need for significantly greater cooperation and technology development in information system defense.

PRIORITY THREAT SCENARIOS

IT-1. DISINFORMATION

As the dependence on information increases, so do the vulnerabilities to intentionally false information. From actual feints and fakes in battle to false real-time intelligence data, from falsified financial transactions to false press releases, data that resembles true data, but is designed to mislead for malicious and hostile purposes is not new; but as information dependence increases, disinformation will become a more powerful weapon.

The immediacy of electronic information can stimulate action long before authentication and verification can be obtained. Strategic and military operations have long required both verification and high-level authorization before action or response. With the proliferation of electronic information systems into every aspect of human interaction, trust and vulnerability have replaced caution and hard verification in many situations. If financially damaging information is released, those effected may have to act defensively (sell), thus exacerbating the situation, before they can verify the negative news. A slightly less urgent scenario would be the news that a disease outbreak has occurred; but here as well, immediate containment precautions would be seen to "confirm" the outbreak before it can be confirmed and defined.

Authentication and verification tools for data are as yet not widely used outside of the banking and national security communities. Encryption might provide some of this capability, but encryption has its own security downside in cloaking illicit and hostile activities.

Adversary Weapons and Tactics

• Increase the fog of war; unleash coordinated multiple false informations; upset the adversary's timing and coordination; provide misleading information immediately before attack; trick battle field sensors; provide credible false information timed to be unverifiable within the response time, out of phase with the observe-orient-decide-act military command loop; undermine inter-unit and inter-Service trust with erroneous harmful information or apparent system information incompatibilities.

- Target single point information sources; target the decision-makers and commanders, who are single-point information failure nodes.
- Corrupt records: intelligence, financial, medical; hide the fact of corruption.
- Corrupt voting processes and data.
- Discredit true sources; reinforce fantasies.
- Manipulate public information imagery; discredit and falsify visual "data".
- Defeat attribution and accountability with anonymity and untraceability.
- Plant ambiguous information, but deny innuendo; use the unretractability of released news.

IT-2. FINANCIAL DESTABILIZATION

One threat fantasy is a massive information assault on the financial world causing instability on the scale of 1929. Open financial data sources of all kinds, financial espionage, and better economic models give perpetrators new advantages. The new electronic wealth, both in the sense of e-companies with huge market valuations and in the lack of hardcopy certification for many transactions and assets, creates new potential for information destabilization and wealth evaporation. While a global scale disaster caused by coordinated corruption of global financial information is not credible, large scale local instabilities might be achievable.

While it is true that e-attacks would backfire on the attacker who is, after all, in the same global economic community, that rogues are less connected into this financial world and therefore might find it harder to understand and access its vulnerabilities, and that economic models have difficulty simulating the complex self-compensating inter-relatedness of market actions, and therefore are difficult to use in pinpointing truly destabilizing singularities, never the less, actual attacks on the financial community coupled with other forms of terrorism and disinformation might create chaos and loss of confidence on a wide and prolonged scale, and might enhance truly negative financial conditions.

Adversary Weapons and Tactics

- Start with latent, graded, many aspect, distributed attacks on the financial infrastructure; hide the extent and scale of the attack until it has become apparent.
- Identify through economic system simulations 2nd and 3rd order financial instabilities; trigger and enhance these instabilities; cause runaway; disrupt synchronization of financial processes and data

transfers; use round off and other numeric schemes to confuse calculations and account balances.

- Disrupt the Federal Reserve clearing process through denial and diversion attacks and corruption of accounting software and data.
- Destroy personal financial records in institutional and personal computers.
- Steal and reuse identities to create confusion.
- Plant programmable Trojan agents designed to corrupt data and processing in accounting and transfer hardware and software.
- Propagate false financial data and rumors timed to be unverifiable; get inside of the financial management response loops.
- Subvert the response process and frustrate cooperative attempts to recover system control.

IT-3. C4ISR FAILURE BY THE MILITARY (Same as MIL-1)

This threat scenario, discussed at length during the Military Technology Workshop, came up again in this Information Technology Workshop, with a partially different set of participants. The summary given in MIL-1 combines the essence of the two discussions and will not be repeated here.

IT-4. CRITICAL GLOBAL INFRASTRUCTURE ATTACK (See MIL-3)

The invasiveness of information systems into public infrastructure sectors, the availability of public information about all sorts of public infrastructure systems, and the ability to manage complicated attacks using networks suggest that infrastructure attacks should be feared. The lack of such attacks to date is surprising. Perhaps, like denial of service attacks, these belligerent acts will come, possibly in the serious context of warfare or a tapestry attack. Or, perhaps, they are more difficult to execute than we have thought.

Adversary Weapons and Tactics

- Attack information and control dependent transportation systems, such as BART and Air Traffic Control; coordinate with physical attack on transportation centers and fuel supplies.
- Attack electric power control and distribution; cause system and customer damaging surges and outages; deregulation has decreased system margins; attack under stressed conditions.
- Attack e-commerce with information weapons. (See IT-2.)
- Attack US global communications using information weapons.
- Use arson and chemical substances to attack information (server and storage farms) and infrastructure systems and personnel.
- Attack information workers; create a fearful and dysfunctional information work force.
- Use required public regulatory reports to identify system vulnerabilities.

- Gain information systems access through back doors designed for system maintenance; remote system management often provides remote access and enables attack.

IT-5. FAILURE OF CYBER POLICY AND LAW

Current cyber law and law enforcement are inadequate to protect the public and the government from crime and terrorism in cyber space, currently so and uncertainly so in the future. This is due to: the continual newness of cyber innovations and practices with many activities legally unprecedented and unregulated; the lack of critical technical means to support law enforcement, indeed with some useful technical capabilities like encryption impeding law enforcement; and the heretofore intentional policy of freedom and lawlessness of cyber space to enable the explosive growth of its economic and social benefits. Some fear that cyber criminals and sociopaths will not only thrive in this gap in societal control, but that their practices will diminish public trust and broadly degrade communality. Others fear that coordinated efforts by national adversaries might use this opening to do insidious harm to us and to gain their own economic and political advantages. On the other hand, many thoughtful people and the general public seem more inclined to let governance of cyber space evolve more slowly, at a pace set by experience, even if that pace seems always well "behind the power curve" and if some of the learning experiences are intensely negative.

Adversary Weapons and Tactics

- Cause disaffection with government and the legal system by using their slow, costly, bureaucratic responses to enable agile crime and frustrate its prosecution.
- Cause the US to over-react, to over-regulate, and to lose both its ability to innovate and its economic competitiveness.
- Incite the cyber have-nots to rebel by taking advantage of their naivete in cyber space, through cyber scams, hit and run cyber crimes, and political and economical influences advantageous to the cyber adept; use the lack of personal protections and privacy in cyber space to achieve illicit economic and political advantage.
- Use the technical advantages of cyber technology for unintended purposes: cryptography to prevent monitoring and forensic access, wireless units to locate, surveil, and eavesdrop on the users.

IT-6. GLOBALIZATION ERA INTELLIGENCE AND RESPONSE FAILURE

Globalization includes not only the diffusion worldwide of advanced technology, but wealth generation and power growth in many new locations and forms among people with a wide range of motivations. We can fail to comprehend the emerging geopolitics and fail to respond appropriately, because we do not have the right intelligence or response tools.

While powerful nations will continue to dominate, active threats and actual conflict may arise from less likely and more distributed entities, such as emerging nations, affinity and terrorist groups, and organized crime. Because the scale of the activities of these entities is smaller and the signatures of information age forces are not those of traditional military forces and facilities, new models and intelligence gathering techniques are needed, techniques which are more intuitive, holistic, and distributed, which can discern the emergence of disparate (geographically, economically, politically, conceptually), but related activities and ideas. Open source intelligence, cyber profiles, and transaction analysis to recognize hostile activities and to identify countermeasures would be of great value in dealing with these non-traditional threats. Conversely, these threats will intentionally show signatures which do not fit traditional experience.

Similarly, traditional military dominance can be both physically and politically inapplicable in combating these threats, because the threat sources are asymmetric to us (do not mirror us), distributed, and imbedded in innocent surroundings. Countermeasures using information weapons and tapestry strategies, for example, may be much more appropriate than aircraft, missiles, and even the most advanced military tactics in dealing with these new global adversaries. Conversely, these adversaries will use asymmetric tactics and may choose to operate boldly where we have little perceived national interest, for example, in Africa or the Asia-stans.

Adversary Weapons and Tactics

- Distribute hostile activities.
- Use information weapons and tapestry tactics.
- Use COTS space technology and global system assets.
- Avoid concentration of active facilities and infrastructure; use existing COTS infrastructure (disinfrastructurization).
- Operate anonymously and through intermediaries.
- Use unfamiliar, innovative, breakout technologies.
- Use out of band and hyper-spectral systems.
- Operate under circumstances ill matched to our military capabilities and deployment practices.
- Take advantage of our intelligence blind spots and operate in modes not recognizable as hostile by traditional signatures.

IT-7. LOSING TO SUPERIOR COGNITIVE COMPUTING

Several trends are converging on a radically new computation mode, cognitive computing, in which the computer acts more like a human intelligence, but with far greater speed, memory, and bandwidth. It is estimated that without dramatic changes in architecture, supercomputers operating at petaflop speed, soon to be available, can simulate capabilities of the human brain. At the same time, neural science is approaching the molecular scale in understanding of the brain's chemical and architectural structure, and organic and electrical operation. It is likely that this knowledge will influence and make more efficient the coding and architecture of cognitive computers. Finally, organic, inorganic, and combination sensors, transducers, and actuators will make computers more able to sense and integrate their own data and produce effects, that is, to perceive and act autonomously.

Given the nature of other threats identified herein, namely, tapestry attacks and globalization emergent adversaries, which require complex holistic conceptualization and execution on the one hand, and gestalt level recognition and countering on the other, it would seem that cognitive computing might signal the next leap forward in the global dominance.

In addition, this capability would be a great advantage in intelligence data analysis, where patterning, conceptualization, and interpretation are currently limited by human capabilities. In particular, such a capability would be ideal for open source intelligence mining, due to the massive amount of data and the unprescribability of intuited intelligence.

COTS computing technology is approaching the cognitive threshold. The IBM Blue Gene machine will operate in the petaflop range. Neural simulation is steadily improving. Chess programs, computer trading, economic models, and the best search engines all perform forms of conceptual activity. The breakthrough to cognitive computing should occur in the next two decades, giving significant new power to its possessor.

Adversary Weapons and Tactics

- Use intelligence in preference to force.
- Use cognitive methods for intelligence analysis.
- Use cognitive methods to maximize effect of tapestry attacks.
- Use cognitive methods for technology and operational innovation.
- Use cognitive analysis for economic modeling and prediction; for designing economic disruption.
- Use cognitive machines to enhance man machine interaction and enhance human performance; shorten human learning time by reducing what the human agent has to know to act through a cognitive interface.

IT-8. EMPOWERMENT OF ADVERSARY GROUPS

Metcalfe's Law states that the value of a network increases as the square of the number of nodes. The power of the individual who uses this exponentiation is similarly leveraged, by organizing with others who reside on the network, by promoting and refining his agenda, by sharing techniques and developing resources, and by managing networked attacks in real time, like those on the meetings of the World Trade Organization. He can act alone or in concert anonymously from an untraceable location at very low cost with relatively little risk to himself or his minimal assets. He can build political support via this medium. He can manage group activities, protests, and attacks. And he can disappear without moving.

Adversary Weapons and Tactics

- Develop and distribute political messages; coordinate influence of public opinion.
- Coordinate affinity groups.
- Raise funds and share assets with affinity groups.
- Hack globally with agility, ubiquity, and anonymity,.
- Penetrate C4ISR and infrastructure controls.
- Use hostile cyber agents: viruses, worms, Trojan horses, denial.
- Coordinate insider threat and insider teams; insiders can bridge security gaps and invade inner sanctums.
- Coordinate financial, infrastructure, and tapestry attacks. (See IT-2, IT-4, and MIL-3.)
- Achieve millions-fold impact at low physical and financial cost.

INFORMATION TECHNOLOGIES WITH THE GREATEST THREAT POTENTIAL

1. Tapestry Attack Simulation Model. A simulation which modeled the operation, functional relationships, timing, and control for the activities of a city, region, or whole country, or for any distributed systems or functions would be very useful for planning the disruption or destruction of these entities with maximum efficiency and impact. Modeling of stress propagation, of responses and response destabilizations, and of cascading effects could be used to increase the catastrophe and even to focus harm. Such a model would be useful for real time interpretation of damage assessments and to manage an attack as well as to plan and manage defensive responses.

2. Computer System Attack Technology. Hardware, code, and procedures for the invasion of information and computer systems for taking, modifying, or destroying information or code, destroying systems, planting agents, listening, locating system elements, or attacking system operators.

3. Tactical EMP. Devices that can generate electromagnetic pulses locally or remotely to disable operation or destroy electronic components, either electrically, thermally, or by intense high energy radiation. COTS computer elements are not hardened, are in fact very fragile electrically. EMP can be enhanced or replaced by straight forward explosive destruction.

4. SIGINT Collection Technology. Remote and local devices and systems for listening, patterning, traffic analysis, and false signal injection.

5. ASAT Against Sensor, Navigation, and Communication Systems. Most commercial and many military satellites are not hardened and are easily destroyed either kinetically or by intense radiation or directed energy, thus disabling global systems for C4ISR, and commercial communication and navigation.

6. Cyber Anonymity, Deception, and Concealment. Techniques for disguising the perpetrator, hiding his cyber path, camouflaging his agents, and impersonating innocent or friendly parties enable stealthy and anonymous information operations; packet ID deception; use of multi-leg, multi-path hopping, and intermediary prepositioned Trojan horse agents.

7. Jamming. Signal and noise saturation, false signal injection, and desynchronization of up- and cross-links, sensors, and communication, computation, control, navigation, targeting, acquisition, tracking, and countermeasure systems.

8. Reconnaissance Imagery. Currently inexpensively available commercial imagery exceeds in resolution and currency thresholds that are a threat to our national security, and these services will improve in resolution, timeliness, and spectral coverage in the future.

9. Micro Power Sources for MEMS. Micro-electro-mechanical systems (MEMS) have achieved incredible feats of computation, sensing, transmission, transduction, actuation, transport, and chemical and biological analysis, but have been limited in usefulness by the lack of power sources reducible to the same scale. The invention of high energy-density micropower sources will be the enabling breakthrough technology for MEMS.

10. Encryption. Encryption is a tradeoff between COMSEC and SIGINT, an ensurer of transactional integrity and security, but a cloak of secrecy for the adversary. The state of the encryption art will advance with computer power and transmission bandwidth. The terminals will remain the points of weakest security.

11. Locators for Wireless Devices. An advantage for navigation and force management, this technology is a problem for networked forces that want to be mobile and hidden.

12. Cognitive Computing. A breakthrough in cognitive computing would revolutionize intelligence, strategy, problem solving, innovation, and man-machine interaction to the great advantage of its possessors.

13. Covert Communication Hardware. Covert operations need communications systems with low probability of detection and interception, and with high reliability.

UNCERTAINTIES

1. Degree of Military Success with Information Technology.

Will the military find a way to acquire and successfully and securely use innovative IT technology? What will be the balance for the military of IT benefit and vulnerability; will advanced information systems be easier to attack than to use?

2. Micropower Technology.

Will it be invented and will the full potential of MEMS be realized?

BIO TECHNOLOGY
WORKSHOP SUMMARY

On October 17, 2000, a one-day workshop focused on threats that are enabled by bio technology was conducted. The participants in this workshop represented the Livermore Laboratory, the US Navy, defense, intelligence, and arms control analysts, Senate technical staff, biologists, bio-technologists, the medical profession, and the bio-technology and defense industries. The following brief summarizes our findings.

PRIORITY THREAT SCENARIOS

- **Agricultural attack**
- **Psychological biological warfare**
- **Emerging and reemerging diseases**
- **Vulnerable population concentrations**
- **Neo-viruses and neo-bacteria**
- **Bio regulation: attack on human performance**
- **Ethnic/demographic bio weapons**
- **Bio hacking**
- **"Righteous" biological warfare**
- **State promotion of biological improvement**
- **Bio - nano - cyber weapons**

and at some point

- **Genetic engineering of animals and humans: neo-metazoans**

TECHNOLOGIES WITH THE GREATEST THREAT POTENTIAL

- **Genetic codes of viruses and bacteria**
- **Human genetic codes**
- **Genetic codes of food crops and animals**
- **Human bio regulation chemicals and pathways**
- **Computational bio databases and codes for analysis and synthesis**
- **Combinatorial organic chemistry**
- **Genetic engineering capabilities**
- **Bio hazard laboratories and field sites**
- **Bio weaponization**
- **Simulation models for bio weapon operations**
- **Nano engineering and fabrication**

UNCERTAINTY

- **Limits on the accessibility of bio information and bio research: regulation, industrial secrecy, and belief constraints.**

INTRODUCTION

While the participants in this Workshop expressed considerable concern about the use of virulent pathogens by terrorists and warring nations, there was broader and deeper concern about the intentional and unintentional consequences of the genetic revolution that is just beginning.

Biotechnology has made tremendous advances in the last decades of the 20th Century. These advances have come about through the technologies of recombinant DNA research, genomics, and proteomics. The results have been rapid and have provided immediate and powerful tools to diagnose human disease and, in some cases, have provided clues to amelioration or cure. We fully anticipate this molecular, genetic, and proteomic revolution to continue in the 21st Century and further enhance the quality of human life.

However, these same technologies that provide enormous benefits to mankind can also be abused or misused. This conference examined some of the issues that might follow from such misuse, accidental or intended. These future (and already emerging) capabilities would both increase the range and lethality of current bio threats, and would enable significant new types of bio threats.

Agricultural genetic modification has been underway for centuries (breeding) and for over a century on the basis of biological science (Mendel); it has been publicly acceptable, and is accelerating, particularly in China. It is feared that surreptitious malicious modification might be used as a strategic weapon, or that well intended modification might have long-term and widespread undesirable side effects.

As we learn to genetically tailor antibiotics, anti-virals, anti-carcinogens, and anti-all-variety-of-undesirable-health-conditions, we strike the Faustian bargain that yields as well all of these same forms of malicious tools: super viruses and bacteria, subtle carcinogens, and attribute-selective (ethnic) and other forms of life and performance degrading pathogens. These pathogens might lie outside of the immuno/metabolic defenses of current life forms, and could cause wide destruction.

But the most profound threat is that we are approaching the era of human control of future bio forms. From genetic eugenics to animals with implanted human genes to the general ability to combine and modify species at the genetic level, we are learning that all life forms are assemblages of genetic parts that we might be able to mix and modify to suit our purposes.

This knowledge and the equipment needed to accomplish such changes will be ever more widely available, and outside the control of authorities, analogous in some ways to the spread of information capabilities in the current information revolution. Indeed, biological commerce will globalize, enabling worldwide benefits, and opportunities for bio hacking, bio crime, bio terrorism, and bio warfare.

These changes will come, are coming, very quickly, within the two decades of this study. Already many of the virulent bacteria and viruses have been genetically decoded and the first genetically designed antibiotic has been tested. These developments are driven by economics and by utility, not by any national plan or moral value. We are initiating a new biosphere in a very ad hoc fashion. Whereas nature has always tested its mutations against all other elements of the mutant's habitat, we have and will develop mutants that are optimized in one dimension, to produce more and better food or medicines or human compatible organs or function-specific organisms or even super humans, athletes and geniuses. These species will be out of equilibrium with their environments, thereby either dominant or fragile, but ecologically unstable.

The values, responsibilities, and mechanisms for guiding US bio policy and activities are lagging far behind the scientific and technological advances. Even the immediacy of national defense has not motivated coherent action. The responsibility for bio agent detection and response lies with the Department of Health and Human Services, while the DOD, FBI, CIA, and FEMA all have overlapping responsibilities for anticipation and response to acts of bio crime, bio terrorism, and bio war. A more coordinated institutional arrangement is needed for prevention of and response to immediate, fast-acting threats. In the longer term, a National Advisory Council on Biology might be commissioned for ongoing study and guidance of US policy, defense, and R&D programs.

PRIORITY THREAT SCENARIOS

BIO-1. AGRICULTURAL ATTACK

Both animal and crop agriculture are becoming monocultural, with single species being selected and genetically improved to optimize the quantity and quality of their product. In addition, these species are being cultivated in habitats that used to be wild and bio diverse. The loss of diversity and focus on single species greatly increase bio risk and vulnerability, and limit nature's or our ability to respond to an assault, even if the assault is natural or unintended.

Monocultural agriculture also assists an adversary who can reach a greater portion of our food resources and population with fewer weapons. Such an adversary might attack a crop to deprive us of food or gain an economic advantage, or might imbed in the crop pathogens (carcinogens) or bio regulators, the effects of which can be subtle and durable, as descried below (BIO-6). The bio agents might be simple contaminants, alien microorganisms or competitive or damaging species, genetic modifications or modifiers, or binary agents, which prepare the crop for the action of an activator agent, which might be used later in the food growth or production cycle, or on the consuming population. These agents could be introduced in the seeds, from the air, through the irrigation water, in the animal feed or crop fertilizer or pesticide, or during the food processing.

Adversary Weapons and Tactics

- Learn the genetic codes of food crops and animals.
- Develop bio weapons lethal to agricultural monocultures.
- Develop bio regulators which can be imbedded in vegetable or meat crops.
- Develop inheritable direct or binary weapons specific to these crops.
- Develop distribution techniques for seed, air, water, or food processing.
- Use conventional agro weapons such as wheat rust, and foot and mouth disease.

BIO -2. PSYCHOLOGICAL BIOLOGICAL WARFARE

Psychology can assist and enhance biological attacks. The impact of a real biological attack or outbreak is greatly enhanced if the disease is horrific, such as the hemorrhagic diseases that end in massive bleeding, or even the black plague or smallpox with their disfiguring symptoms. Panic can cause infected people to flee and spread their disease. Intemperate news coverage can incite panic; in fact, the media and the Internet can be used to create public dysfunction and impede appropriate response. Terrorists or extortionists can use natural outbreaks by claiming to have initiated them, and by threatening more outbreaks if their demands are not met.

Economic damage and social dysfunction can be caused for at least a limited time by fear alone. There is a crisis about genetically modified corn in the US, Japan, and Europe, not that it has caused any harm, but products made from it are being removed from the store shelves. Apples sprayed with Alar and strawberries genetically protected against frost were not allowed to be sold, although only fright, no actual harm had come from them. This fearful, closed attitude about "unnatural" food technology, the distinction between breeding and grafting versus chemistry and genetic engineering, can be used to an adversary's advantage by destroying competition in the marketplace and by gaining international advantage, as China aggressively pursues agricultural modification, while Europe is restrained by popular fear of these methods and products.

Adversary Weapons and Tactics

- Promote distrust of bio technology.
- Discredit health authorities.
- Amplify crises with exaggeration and false reports.
- Credit terrorists for natural outbreaks.

- Subvert response to real attack with disinformation and misdirection.
- Coopt the media and the Internet for the above purposes.

BIO -3. EMERGING AND REEMERGING DISEASES

The 1918 influenza epidemic killed nearly 21.5 million people and sickened nearly a billion. The recent outbreak of ebola in Gulu, Uganda, and of West Nile virus in New York City evidence the continual emergence and propagation of disease among the increasingly mobile global population. In March 1999, a new strain of the Hendra Encephalitis virus hit the Malaysian state of Negri Sembilan, decimating the region's pig population. The epidemic forced health authorities to cull in excess of 800,000 pigs, with officials vaccinating another 500,000 in an attempt to control the spread of the disease. Malaria is persistent and tuberculosis is increasing. 17 million die worldwide each year from infectious diseases.

Diseases like smallpox, which have been eradicated, but which exist in laboratories and for which the population is no longer immune because vaccinations have worn off and vaccination supplies are scant, represents a terrifying warfare and terrorism opportunity. The global population is again vulnerable to a smallpox epidemic.

The imprudent use of antibiotics in humans and animals is blamed for enabling mutation to produce resistant bacteria, which now infect our hospitals and account for as many as 100,000 deaths in the US each year.

It has recently been hypothesized that modern hygiene can create vulnerabilities by preventing the exercise of our natural immune systems because our environment is too sterile. This is proposed to be one reason for the remarkable increase in asthma and allergy incidence and severity.

Finally, global warming might promote disease incubation and vector spread. Initial simulations indicate changes in disease location, but no notable increase in occurrence. One might even be concerned that global environmental changes will cause modified life forms and new microorganisms, viruses, and bacteria.

Adversary Weapons and Tactics

- Inject emergent diseases into US habitats.
- Import vectors into the US.
- Restart smallpox.
- Introduce antibiotics into incubation environments (sewers) to breed resistant bacteria.
- Use modified diseases to improve their survivability in US environments.

BIO -4. VULNERABLE POPULATION CONCENTRATIONS

Today's mega cities make ideal targets for biological attack, with extremely high population density, extremely crowded transportation terminals, subways, and vehicles, buildings with completely enclosed air circulation systems, and single sources of water. These cities are often accessible from the sea, even down wind from the sea, like Los Angeles, New York, and Miami, Hong Kong, Shanghai, and Bombay, and most of Taiwan. Geographic vulnerability distinguishes these potential bio targets, but such actors as the drug subculture and the homeless population in cities can also increase the cities' disease susceptibility. The annual prevalence of flu in cities, even with widespread inoculation, is indicative of this vulnerability.

Israel is in constant jeopardy of a bio assault, but is very wary, and as well prepared as it is possible to be with current means; but that is not to say that heavy casualties could be prevented. It is probable that an attack of this sort would jeopardize the Palestinian population more than it would the Israelis; and the likelihood is high that the effects would spread to the surrounding Arab world, and possibly much further.

Adversary Weapons and Tactics

- Use the natural environment (wind, rain) to distribute pathogens in cities.
- Attack cities where diverse diseases already exist and might initially conceal the new onslaught.
- Use migrant populations to inject disease.
- Use the drug culture and vagrant populations to spread disease.

BIO -5. NEO-VIRUSES AND NEO-BACTERIA

As the genomes of viruses, bacteria, and the high level life forms are decoded, knowledge of pathogens' precise methods of attack will be learned and the possibility of designing pathogens specific to the DNA of the target species and immune to antibiotic and other defenses will be realized. The mechanisms by which other diseases, such as cancer, infect and propagate, forming and using protein agents, will be known, by virtue of having found the mechanisms for curing these diseases. 800 gene therapies are currently in clinical trials. And, finally, the repertoire of the bio weapon designer will be virtually without limit, because the capability to conceive ab initio at the molecular level the means to attack any microbiological function will be available.

Initially, viruses and bacteria will be altered one codon at a time to "walk away from their antibodies and vaccines." (HIV has 9 genes and 10,000 codons.) Combinations of pathogens (for example, viruses that cause cancer) will be produced, which combine their lethal effects and increase the complexity of immunizing against them. Genetic shuffling among bacteria will be used to create countless new varieties. And combinatorial chemistry will be used at a finer scale to optimize the desired characteristics. The incubation time, symptoms, infectiousness, and terminal phase of the infection will be of the designer's choice.

Hopefully, generic pathogenicity detectors and generic antibodies will also become available. Where there is money to be made, there will be enormous efforts to develop pharmaceuticals and industrially useful microorganisms, which will generate knowledge both of the organisms and of the methods to render them safe for commercial use. This same knowledge could yield new biological weapons. The power of genomics based supercomputation could be turned from analysis to synthesis of such weapons.

Adversary Weapons and Tactics

- Obtain genetic databases, analysis codes, and laboratories for virus and bacteria modification; this might be concealed in a pharmaceutical facility.
- Use public international scientific information resources.
- Access computer resources under academic cover.
- Promote and fund legitimate research foundational to this purpose.
- Access pharmaceutical and chemical industry research data.
- Access the bio hacking community.
- Test neo-pathogens in the laboratory or in the public.
- Execute non-attributable attacks on US populations, such that they are not distinguishable from natural outbreaks of mutant pathogens.

BIO -6. BIO REGULATION: ATTACK ON HUMAN PERFORMANCE

Hormones influence very high level human activities, such as metabolism, growth, and reproduction. They affect energy level, body temperature, mood, attitude, alertness, aggressiveness, and anxiety. They also affect the production of other hormones.

The production of hormones is controlled by various chemical regulators. It is conceivable that an adversary might use such regulators to cause subtle, but very wide spread changes in the capabilities of US human resources and of our soldiers, possibly decreasing our competitiveness, our alertness, even our reproductive rates and the quality of our offspring. Such regulators might be introduced into our population much as biological or chemical weapons are introduced, or by more subtle means in which the agents are imbedded crops and animals.

Such an attack might have no obvious symptoms. We would simply be less capable, less productive, less competitive, less reproductive, more passive, apparently less intelligent. Over the long term, these few percent effects would greatly diminish our global power and influence, and our quality of life.

Conversely, such regulators might be used more directly by adversaries to enhance the performance of their people.

Adversary Weapons and Tactics

- Obtain bio regulation databases, analytic codes, and laboratory facilities; again, university and pharmaceutical research might be the cover.
- Perform tests under legitimate-cover public projects.
- Test enhancements on military and athletic personnel, under legitimate cover.
- Use food and water distribution systems to distribute bio regulators.

BIO -7. ETHNIC/DEMOGRAPHIC BIO ATTACK

Ethnic weapons that target particular sets of people might be either chemically or socially based. With the complete knowledge of specific human genomes, which is becoming available, it will be possible to target specific gene sets with some of the "weapons" described above: neo-toxins, neo-viruses, neo-bacteria, and neo-bio regulators, "neo-" referring here to specifically designed and chemically or genetically engineered pathogens, not naturally occurring.

Two difficulties with this method of attack are (1) that many "races" are actually extremely diverse genetically, for example, Africans who are internally more diverse than their differences from other "races," and (2) that the targeted set of genes might also be characteristic of untargeted populations whose gene sets are not known.

The second form of this sort of weapon is socially based. The African nations and ethnic groups have proven to be extremely vulnerable targets for AIDS. The disease is very slow acting, with no immediate symptoms, and bodily-fluid contact contagious. The invisibility of the disease, lack of social rigidity, family separation due to remote work and military service, and the lack of health education and health resources prevent effective control. If one were to design a biological weapon against these people, AIDS would be an optimum choice. Whereas, it is less widespread and lethal in other cultures.

Smallpox is purported to have been intentionally used in the French and Indian War by the British against Native Americans, who had no knowledge of or defense against this disease.

Adversary Weapons and Tactics

- Obtain the genome codes for the target groups.
- Develop neo-pathogens targeted to that group, but not harmful to the other or the attacking group.
- Design the pathogen to work selectively with the cultural habits of the target group.
- Perform natural-outbreak covered trials within the target group.
- Optimize the pathogen cycle for the target group.
- If possible, disguise the neo-pathogen as a natural mutant to hide the attack and frustrate attribution and medical response.

BIO-8. BIO HACKING

Some of the bio chemical and genetic manipulations described above will be performed using relatively simple equipment. The data bases and calculational tools for molecular starting points and molecular manipulation are already becoming widely available. Bio hacking, the popular and mischievous pursuit of genetic engineering, will undoubtedly obsess bright, amoral, bio gamesmen, unleashing a far more lethal form of analytical adventurism than cyber hacking.

These "terrorists" will be less likely to be as careful and experimentally rigorous as institutionally supported researchers, which will increase the probability of accidental events from the hackers. This group might also include disgruntled employees of chemical and pharmaceutical companies where vastly more data, instruments, and synthesis tools will be available to them.

In addition, the ability to make mind altering drugs and bio regulators will enable the design and production of a wide range of recreational "organic drugs." In the very long term, this group might also modify species, invent a pet, and create "interesting" metazoans (BIO-12).

Adversary Weapons and Tactics

- Promote interest in bio hacking among relevant affinity groups.
- Promote bio script development and sharing.
- Enable hacker access to super computer resources and laboratories through legitimate education and research channels.
- Encourage the academic community to be open to this group.
- Assist this community with relevant, but disguised weaponization information.
- Publicize bio hacking achievements and adventures.

BIO -9. "RIGHTEOUS" BIOLOGICAL WARFARE

It has been seriously suggested within the US government that we engage in biological warfare against coca crops in Colombia, that we alter the chemical environment or release a targeted pathogen to kill the coca species there. After all, such a dire approach might be justified to "win the war on drugs." Such a rationale might be extended to other species, such as malaria carrying mosquitoes (which we already attack by distributing sterilized populations of their species to inhibit reproduction), plague carrying rats, the grape destructive glassy-winged sharpshooter, and even tobacco and marijuana.

By extension of this rationale, we might use bio regulators or more toxic and targeted bio weapons to ward off invaders of our homeland. If this were our declared policy, it might act as a deterrent against potential adversaries. It should be pointed out that this logic is not dissimilar from our nuclear deterrent policy, and that the consequences might be unpredictable and similarly dire.

Perpetrator Weapons and Tactics

- Develop neo or natural pathogens which target the offending flora or fauna.
- Declare intentions and attack openly.

BIO -10. STATE PROMOTION OF BIOLOGICAL IMPROVEMENT

As the global bio era emerges, there will be nations that are bio haves and others that are bio have nots. Those nations which engage the bio revolution with rigor and discipline should gain significant economic, ecological and health, and security advantages. On the one hand, thorough analysis and testing with adequate time to observe consequent effects of bio innovations are prudent before human or animal or crop species are exposed. On the other, inordinate caution might well be disadvantageous. Europeans, particularly the French, are very cautious, even predisposed to reject genetic modification of food sources; China is very aggressive, even adventurous with regard to genetic modification of crop and animal species, and to human performance enhancers; the US is moderate in policy and public acceptance, but appears to be moving toward the European position. It remains to be seen which course succeeds best in the long term.

Adversary Weapons and Tactics

- Encourage bio modification and species improvement through government sponsored research.
- Enable rapid commercialization of resultant products.
- Use nationalism as one motivation.
- Use all open scientific sources.
- Test advances in direct international competitions.
- Conceal as much of the program as possible from foreign intelligence.
- Protect advances from foreign exploitation and commercial adaptation.
- Adapt advances to military, as well as civilian use.

BIO -11. BIO - NANO - CYBER (BNC) WEAPONS

The convergence at the molecular scale of biological, mechanical, and electronic technologies could bring very significant technological advantages. Today, transistors are about 5,000 atoms across; in the future transistors could be replaced by molecules decreasing their linear dimension by about a factor of 100 and their density by 10,000 or more. Living cells will be incorporated directly into chip circuits, acting as sensors, switches, and actuators. Proteins are being used as chemo-mechanical devices.

DARPA is embarking on an array of research programs which will explore the intersection of these three technologies, expecting to find applications as sensors and monitors, actuators and nano-machines, chemical analytic tools, bionic devices, neural/information system elements, and other uses yet to be imagined.

These devices would be of such a small size that they would not need concealment. Or they might be hidden within other man made or living systems. They might be used for intelligence gathering, for networking, as triggers, and as platforms for chemical and biological weapons. Independent means of electrically powering these tiny devices is a significant challenge, although they might be powered from the larger systems in which they might be imbedded. Accessing the power systems of living organisms would be a significant breakthrough.

Adversary Weapons and Tactics

- Use BNC devices as area monitors, sensors, and reporting systems.
- Use BNC devices to gather intelligence.
- Organize local area BNC military networks.
- Use BNC devices to convey and activate chemical and biological weapons.
- Use BNC devices as detector/sorters for the discovery of new CBW.
- Use BNC technology for advanced computers.

BIO-12. GENETIC MODIFICATION OF ANIMALS and MAN: NEO-METAZOANS

The extensive genetic modification and combination of animals and humans will come. Genetic modification and combination of plants is already well developed science and technology. Many gene therapies of human maladies are in clinical trial. The genetically specific, as opposed to bred, modification of animals is also coming. Already human genes have been placed in animals to stimulate the production in the animals of human needed organic chemicals. Animals have been cloned and a company in the Bahamas called Valiant Venture, LTD. is now offering human cloning services, although they have yet to demonstrate this capability.

General eugenics and gene specific eugenics, modification of animals for agricultural, commercial, ecological, or security purposes, and the sharing of human and animal genetic material will soon follow. The time scale of evolution is being compressed by millions and the selection criteria are humans' choices. Greater intelligence and some degree of immortality will result. These implications are larger than the context of national security. The height of this bio wave is not yet imaginable, but the rising edge is here.

Adversary Weapons and Tactics

- Obtain databases of gene locations, compositions, functions, and expressions.
- Design the gene composition for the genome of the desired being.

- Engineer the desired genome.
- Construct the being.
- Grow, observe, test, and iterate.

BIO TECHNOLOGIES WITH THE GREATEST THREAT POTENTIAL

1.. **Genetic Codes Of Viruses and Bacteria.** Mapping and understanding the genomes of pathological organisms and their gene functions, so that they can be countered, or modified for defensive or harmful purposes.

2. **Human Genetic Codes.** Generally, the complete sequence of the genomes of target populations; specifically, the information needed to identify viral and bacterial vulnerabilities or potential vulnerabilities, and for coding the production and function of bio regulators; in general, since we cannot predict what beneficial or harmful mechanisms will be found, the entirety of specific human genomes and of the coded functions.

3. **Genetic Codes Of Food Crops And Animals.** Generally, the complete sequence of the genomes of target crop and animal populations; specifically, the information needed to identify pathogenic vulnerabilities or potential vulnerabilities and for coding the production and function of bio affectors of any kind in these species to influence their growth cycle or characteristics or code genetic information that might want to be passed on to the food consumers for malicious purposes.

4. **Human Bio Regulation Chemicals And Pathways.** The understanding of the direct (drugs) and subtle (hormones, steroids) bio regulators that affect human actions and performance; binary forms of such agents with enabling and activating elements; the possibility of causing permanent physiological or genetic changes that effect personality, performance, or health.

5. **Computational Bio Databases and Codes For Analysis And Synthesis.** Codes and databases for chemical, structural, and functional analysis of genomes, genes, and proteins; the capability to synthesize genetic material for specific biological functions.

6. **Combinatorial Organic Chemistry**. An important subset of the capabilities just described, which enables the computational generation of all possible combinations and permutations of codons for the design of genes, proteins, and bio regulators.

7. Genetic Engineering Capabilities. The means, much of which is available in today's bio-tech and pharmaceutical companies, to manipulate genomes, one codon at a time, or by shuffling genes, and then sort the results with multi array or generic function detectors to select the desired bio functions in the resulting organisms; the capability to produce the desired organisms when they are identified.

8. Bio Hazard Laboratories And Field Sites. Bio material handling and testing facilities that contain the hazardous material during engineering and testing in the laboratory and in a field setting; an essential capability for bio engineering.

9. Bio Weaponization. The ability to stabilize pathogens in a deliverable form, with platforms appropriate to the operation, e.g., aerosols sprayed into a wind or onto the target area or quantities delivered in micro-electro-mechanical devices that activate and release on command.

10. Simulation Models For Bio Weapon Operations. The physical modeling of aerosol dispersal in complex settings from air-, sea-, or land craft into a wind or building air system, or as a fluid into water or food supplies, or in fertilizer or pesticide or steroids, or in widely distributed human ingestives; along with the psychological, economic, and response models needed to optimally phase and distribute the attack for maximum effect.

11. Nano Engineering And Fabrication. The capability to fabricate devices at the cellular and even molecular scale, which combine mechanical, electrical, thermal, fluid and gas, and organic processes, to perform sensory, chemical and bio analytic, computational, information storage and transmission, networking, self powering, robotics, and even weapon delivery and control with other similar devices for bio, environmental, intelligence, and military applications.

BIO TECHNOLOGY UNCERTAINTY

• Limits On The Accessibility Of Bio Information And Bio Research: Regulation, Industrial Secrecy, And Belief Constraints.

The accessibility of bio technology information will be limited by government secrecy in the cases of biological weapon materials, by regulation where products are judged to be too high risk for the benefits or if overly stringent moral standards are applied, and by companies, which want to protect their proprietary interests. Cultural and religious beliefs might also constrain bio innovation. It is not clear that these constraints will be reasonable and beneficial, or reactionary and disadvantageous to the US.

GEO SYSTEMS TECHNOLOGY WORKSHOP SUMMARY

On September 14, 2000, a one-day workshop focused particularly on threats involving energy stored in natural systems and alterable characteristics of the global environment was conducted. The participants in this workshop were affiliated with the US Global Change Research Program, Lawrence Livermore National Laboratory, the Naval War College, New York University, and a defense research center. The following brief summarizes our findings.

PRIORITY THREAT SCENARIOS

- **Water supply destruction**
- **Dam destruction: mega dams and earthen dams**
- **Pathogens in geo systems**
- **Energy and mineral resource denial**
- **Fire**
- **Air and environment corruption**
- **Natural disasters: tsunami, hurricane, torrential rain, drought, volcano, earthquake, asteroid**
- **Sharp geo-social gradients**
- **Electromagnetic disruptions**
- **Critically vulnerable localities (e.g., New Orleans, Venice, Bangladesh)**
- **Triggers and modifications of geo systems**
- **Land and ocean food supply destruction**

TECHNOLOGIES WITH THE GREATEST THREAT POTENTIAL

- **Nuclear weapons**
- **Biological pathogens**
- **Genetic modifications**
- **Chemical and heavy metal poisons**
- **Radioactive contaminants**
- **Conventional explosives**
- **Fire igniters**
- **Fuel storage facilities**
- **Atmospheric composition modifiers**
- **Earth albedo modifiers**
- **Ocean surface modifiers**
- **Methane hydrates and carbon dioxide in deep waters**
- **Coupled models of geophysical phenomena at all scales**

INTRODUCTION

Geo systems, such as weather systems, ocean currents, crustal formations, and bodies of ice and water, are huge in scale and contain prodigious amounts of energy. For example, a large hurricane releases as much energy as a 1-megaton explosion roughly every 10 seconds (and the very largest every 1 second or so); a large earthquake releases the energy equivalent of 10 million megatons of explosive.

As models of and data on these systems improve, the ability to predict what will, or even might, happen will improve. Such knowledge could offer both a competitive and a self defense advantage. The means may even emerge to modify, initiate, and redirect the energy contained in these systems by means of very high gain trigger or boundary condition mechanisms. Myth has it that before these systems become mighty, the flutter of a butterfly's wing can set them in motion. Of course, it is also argued that many coherent mega-butterflies are needed, and that the chaotic nature of natural systems makes the effect that they trigger completely unpredictable.

As society develops and becomes dependent on global intercouplings of products, infrastructure, information, and travel, natural events can cause significant disruptions of societies and the economy (e.g., the drought, fires and economic collapse of economies in SE Asia) that can have ripple (or even tidal wave) effects around the world. The large energy release and disruptive influences can be attractive to terrorists.

The atmosphere-ocean-land system is also the underpinning for the biosphere. Changes in the geophysical environment can determine the viability of living things and the course of evolution. The ability to modify or corrupt these vast systems or their local eddies could greatly impact our security.

The world is changing as a result of human actions: much of the world's land cover is changed, atmospheric composition is different and climatic change has begun, stratospheric ozone has been depleted, and more. We are not yet able to fully predict the consequences of these changes and are only starting to build the commitment to limit their influence. Over time, increasing information and insight will emerge. Having that information is likely to affect the balance of advantage among nations, and we need to be sure we are the best informed.

PRIORITY THREAT SCENARIOS

GEO-1. WATER SUPPLY DESTRUCTION

Water is in diminishing supply relative to demand, is a resource that is often to be shared or fought over by several claimants, is the collector and distributor of toxics and alien species, and is the potential distribution system for intentional harm.

In general, available water is being put to full use; there are shortages of supply in most places, obviously, in desert areas, but increasingly in cities and areas not regarded as drought vulnerable. Cities, such as Albuquerque and Los Angeles, depend on aquifers, which they are drawing down with resulting diminishment in quality and eventual scarcity; these aquifers are already contaminated with hydrocarbons and salt, respectively. A rising sea level threatens coastal aquifers with salinization in a number of other areas. While El Paso has adequate aquifer supplies and manages its water carefully, the cross-border city of Cuidad-Juarez is depleting its aquifer supply, and this city of over a million people may run out of water in decades, creating water refugees. Israel, Jordan, and Lebanon share aquifers that they are depleting, a politically dangerous trend. New York City draws water from plentiful upstate surface sources, but at such a prodigious rate that if the supply were interrupted, the city would run dry in only a few hours. A recent survey of American cities found many water supplies failed required health standards. City water supplies are under stress and thereby vulnerable to physical and biological attack.

River resources flow through many nations, which, as globalization increases the demands, will become more valued and coveted for agriculture, hydroelectricity, and human needs. Most of the great rivers of South and Southeast Asia start in Tibet. The Tigris and Euphrates start in Turkey. The great rivers of central Africa transit many nations. The use of these waters will be sources of contention and their dams will become vulnerabilities as discussed below.

Rivers gather fertilizer and pesticide runoff from agriculture, industrial effluent and waste leach, and spillage from shipping. These foulings damage downstream communities and eutrophy the deltas and coastal waters, creating breeding grounds for disease and destruction of ocean fishing grounds.

Finally, water supplies are a potential distribution system for chemical and biological attacks.

Adversary Weapons and Tactics

- Destroy water distribution systems.
- Divert water from users: Turkey, US, and Zimbabwe can do this.
- Break aqueducts, dams, canals, reservoirs.
- Attack treatment plants or their supporting infrastructure.
- Interrupt industrial processing, fire fighting, air conditioning: 10,000,000 gallons spilled into the World Trade Center in 90 minutes.
- Attack transportation systems beside rivers causing spillage.
- Contaminate water supplies, or simply discredit supplies with false warnings.

GEO-2. DAM DESTRUCTION

Dams are a manmade system that stores huge amounts of releasable energy. Destruction of a dam can disrupt water supplies, irrigation, and electric power, damage the local environment, and take many lives down stream, even destroying parts of cities and the infrastructure they need to be viable (e.g., sewage treatment systems). The Aswan dam has been described as "the Nile in the barrel of a shotgun." Destruction of the Ruhr River dams was devastating to the German economy in the Second World War. The Three Gorges Dam in China will create a whole new class of vulnerability, being the largest dam project by any measure, with the most power generated, the most water stored, and the largest population downstream. It is thought that a few tons of modern penetrating explosive could destroy these dams.

In addition, many earthen dams, much more vulnerable to attack, but storing less energy and depended upon by fewer people with less consequence to their destruction, are much more accessible to harm. Examples are the Teton dams and Dutch and Northern Californian levies.

Adversary Weapons and Tactics

- Lesser dams could be destroyed with one ton of explosive.
- Greater dams would require modern penetrating explosives.
- Generators are the most vulnerable, and could be put out of service with explosives and machine damaging chemicals and gums.
- Destroy dam peripherals: gates, sluices, pipes, storage, and controls, possibly enabling dam topping flows.

GEO-3. PATHOGENS IN GEO SYSTEMS (See GEO-12.)

In the broadest sense, geo systems include not only the oceans, the atmosphere, the surface systems, and the crust, but also the living systems. These include the flora and fauna, but also humans, which are perhaps the most mobile and most widely distributed agents and "vectors". In the past, winds, currents, migrating species, and even crustal movements and climate shifts have carried alien species and bio agents to new environs. Today humans and their transportation systems are unwitting carriers. To date, these biological vectors and pathogens have not been used over large scales as weapons, presumably both because they have been deterred and because the agents tend to be indiscriminant, potentially harming the perpetrator as well as the target.

As technology enables pathogens to be targeted at specific victims, the use of broadcast delivery systems is likely to become more advantageous. Recently, a new antibiotic was developed by designing it to attack a bacterium with a specific DNA sequence. It is probable that bio agents will be able to target not only species, but specific DNA signatures. Such agents could be introduced into large-scale delivery systems (weather, currents, water systems) and they would seek out their targets.

Agents might be designed to destroy local food supplies or even to convert local food and symbiotic species into lethal agents, thereby localizing the effect indirectly, even though taking advantage of global delivery systems.

Local environments favorable to the local propagation of lethal agents could also be created by taking advantage of specific climate and weather conditions. Global changes will have local effects that are amplified and could favor the emergence of either the vector or the disease within a selected locale, for example, increased warmth and wetness creating a malarial zone, or polluted river flows creating a cholera outbreak. Prediction or control of such effects requires high resolution simulations of climate and weather conditions. Under very limited situations, it may also be possible to modify these conditions (e.g., cloud seeding, pollutant release).

And finally, vectors could be transported to local bounded environs that are favorable to them, thus, focusing the effect of the bio agent.

Adversary Weapons and Tactics

- Modify agents to target selected DNA signatures.
- Use geo systems as broadcast distributors.
- Use climate and weather models to define and project favorable conditions for vector and agent distribution.
- Use dispersion models to define vector and agent pathways.
- Use insects and animals as directed local vectors.
- Introduce alien destructive species and vectors in local habitats.
- Use wetlands and other favorable microclimates as incubators.
- Use soil vectors that are slower, but local and less attributable.
- Attack weather weakened species.

GEO-4. ENERGY DENIAL

Hydrocarbon energy sources will become increasingly precious, and will continue to be a source of power for their possessors. We need oil to enable our military forces, our industry, our mobility, our security, and the life quality of our population. We currently use hydrocarbon energy at a greater rate than other nations, but emerging nations such as China are rapidly increasing their usage and are approaching the level of our needs.

The price of oil has now risen back to the levels of the Persian Gulf War. Natural gas is currently in short supply and the price has risen dramatically. Fortunately, the sources of these resources are globally distributed, and the possessor nations need the income from energy sales for the health of their economies. But this market is extremely dynamic and only conditionally stable. If any single major supplier curtails our supply, this is a serious national security issue.

As the Caspian region becomes a major world supplier of oil and gas, it being geographically surrounded by Russia, China, the emerging Asia-stans, and the Middle East oil states, it is very likely that energy motivated conflicts and disruptions will occur here. Long pipe lines run through this region to Turkey to provide Europe and the US access to these energy resources. This is clearly a region of great national security interest to the US, a region in which any of number of states could cause us great difficulty.

Oil and gas will become increasingly dear, and as such, sources of power and threat, as the world's population grows and wealth increases.

Adversary Weapons and Tactics

- Form energy monopolies and cartels to control the price and availability of energy.
- Threaten the energy distribution infrastructure, pipelines, storage, refineries, shipping.
- Disrupt markets in energy using information operation tactics, market manipulation, or source disruption.
- Use environmental mechanisms to impede exploration, field development, and transport of fossil energy.

GEO-5. FIRE

Huge amounts of energy are stored in biomass, both unprocessed (grass, brush, and trees) and processed (buildings, fuel, and hydrocarbon products). Some ecosystems are very efficient in generating and accumulating large stores of high combustibles. Examples include the chaparral that grows over a few decades before burning in hard-to-control fires, eucalyptus and pine forests that store energy over a few decades that becomes combustible during drought conditions, and even new grass species benefiting from higher CO_2 levels. With the right topography and scale, biomass accumulations can be a fire bomb, pulling in fresh air and sending an igniting blast at fresh fuel. Treed neighborhoods of combustible homes, such as Oakland, Los Alamos, Los Angeles canyons, and mountain-side forests are ideal geometries for conflagration. Destruction of the foliage can have the consequent effects of desertification, of mud slides and loss of flood control, and of loss of habitat and species destruction.

Storage depots for oil, gas, liquefied natural gas, propane, and many other fuels and chemicals contain the energy equivalent of many kilotons and liquefied natural gas tankers can contain the energy equivalent of a megaton or more, if they can be air mixed and ignited en masse. Such events could cause detonation and blast effects on the scale of nuclear weapons, if correctly dispersed or aerosolized and ignited.

Fire in confined quarters, such as high-rise buildings or underground facilities, need only generate toxic smoke and gases to be highly lethal. Given concentrations of information infrastructure, single point events can cause disruption over much larger, even global scales.

Modeling and prediction of weather conditions conducive to fire, or disruption or distraction of fire response teams, could be used to design and execute extremely destructive fire attacks.

Adversary Weapons and Tactics

- Take advantage of the energy stored by natural ecosystems and accumulations of processed products (e.g., widespread arson in forested regions).
- Take advantage of the energy contained in stored fuels; use precursor devices to increase aerosolization and dispersal of fuels.
- Use fire to create and disperse toxic chemicals.
- Use smoke, soot, and fire debris to shut down sensitive operations.
- Use models to choose and design fire attacks.
- Model enclosed spaces to increase lethality of fire effects.
- Take advantage of the disruption caused by fires following earthquakes

GEO-6. AIR AND ENVIRONMENT CORRUPTION

Air, liquid, and solid environs can be corrupted to the degree that they pose disabling or lethal threats, either immediately or over extended periods. Examples of contaminants of such potency are: chlorine, as is widely stored and used to sterilize water supplies; industrial gases such as the chemical gas released at Bhopal, India; radioactive contamination, such as occurred from the Ukraine by the Chernobyl explosion; radioactive contamination at waste storage sites in Russia; the potential dispersal of plutonium or reactor wastes (e.g., by attacks on the waste products in transport); the release of tritium into the air or water; the release of heavy metals or endocrine disruptors; the release of chemical or nerve weapon agents; or the creation of smoke from extensive fires. These contaminants are potential weapons.

In addition, the pollution from transportation, heating, power generation, and industrial processes cause slower, but very widespread damage to living things. It is estimated that China suffers a 10% crop loss from air pollution and 100,000 deaths per year from airborne particulate matter; ecosystem damage is also occurring due to acid deposition. China has also suffered greatly from health problems caused by the extensive use of agricultural pesticides, and as a result is embracing genetic modification of its crops to minimize pesticide use. As more nations industrialize, more environs will be subject to these inadvertent health risks.

Adversary Weapons and Tactics

- Use enduring chemical weapons.
- Attack chlorine and other lethal chemical storage facilities.
- Attack radioactive waste storage facilities and nuclear reactors.

- Disperse plutonium, heavy metals, or endocrine disruptors.
- Unmanaged industrial and societal wastes (own worst enemy).

GEO-7. NATURAL DISASTERS

Earthquakes, volcanoes, torrential rain and floods, tsunamis, tornadoes, hurricanes, snow and ice storms, mud and snow slides, and under ocean landslides all have great destructive power. As more becomes known about the mechanisms of these catastrophes, it may become possible to initiate or modify them or redirect their force. Small earthquakes have been inadvertently initiated by the injection of water under pressure during mining operations. Slides and avalanches can be triggered. It is theorized that a tsunami might be caused by a slump of a continental shelf which itself could be started by an explosive or by a destabilization of deep underwater clathrate formations. It is hypothesized that clathrate generated bubbles might be of a scale that could sink ships (Bermuda Triangle). In August of 1986, nearly 2000 people died as a result of a gas release from Lake Nyos, in Cameroon, West Africa. Carbon dioxide had built up in lower waters of the lake and, as a result of a small earth tremor, was suddenly released, causing a cloud of CO_2 to roll down the mountain, killing many people as they slept.

Tsunamis with energy in the range of 10,000 megatons have been triggered by underwater landslide caused by slumps of continental shelves and steep volcanic islands.

Volcanoes near population centers, such as Vesuvius, Rainier, and the volcanoes near Mexico City, have and will in the future cause great destruction if they erupt.

Hurricanes release tremendous amounts of rainfall. Hurricane Mitch inundated Central America with an inch of rain per hour for two days; this storm has caused large-scale movement of refugees toward the US, creating significant border tensions with Mexico. Climate change is projected to amplify wind speed and rainfall amounts from hurricanes. Trends already indicate an upward tick in the frequency of heavy and extreme rainfall events that can cause local flooding. There is tremendous potential energy stored as water vapor in the atmosphere.

Asteroid collisions with Earth could cause regional or global catastrophe, as they have in the past. In the 1908 Tanguska event, an object only about 50 m in diameter caused destruction over a very large area of Siberia; such an event is expected every 100 to 1000 years. About 1,000 objects in dangerous orbits are known to be of sufficient size to cause global scale destruction; the orbits of fewer than half of these are known well enough to predict their interaction with Earth.

Such events unleash vast amounts of energy. While it is unlikely that they can be used as weapons, because the energy required to trigger or alter them is so great, it is likely that they will become better predicted as models improve and the historic data and real time monitors are coupled to these models. And it is possible that triggerable instabilities will be found. Efforts at hurricane modification, both in intensity and direction, have in the past been attempted. They were stopped because of the dangers involved and because of the lack of predictability, a limitation new models may overcome.

Adversary Weapons and Tactics

- Use the advantages afforded by superior catastrophe prediction.
- Take advantage of disaster-weakened opponents.
- Use triggerable instabilities.
- Take advantage of the social disruption caused by natural disasters.

GEO-8. SHARP GEO-SOCIAL GRADIENTS

Geo-physical, economic and demographic, ethnic, and ideological gradients and discontinuities exist that can cause migration, invasion, and conflict. Mexico and the US, Israel and its neighbors, India and Pakistan, China and Siberia, Australia and Indonesia, and Europe and North Africa are examples of such sharp discontinuities. Population, wealth, oil and gas, water, agricultural fertility, religion, culture, and governmental viability are some of the measures of sharp difference.

These conditions are both the indicators of potential trouble and the differences that can be exploited by revolutionaries who promise greater equity or vanquishment of the diversity. Often both human and natural resources are destroyed in the ensuing warfare.

Adversary Weapons and Tactics

- Emphasize the inequity of the differences, and the deservedness of the faithful.
- Extort protection payment or asset sharing.
- Show that the advantaged are vulnerable by initiating the destruction of their assets.
- Capture the advantageous assets.

GEO-9. ELECTROMAGNETIC DISRUPTIONS (See NMS-6.)

In addition to local electromagnetic pulse (EMP) weapons which are directed at or used in proximity to their targets, it is known that a large-scale nuclear device detonated in the upper atmosphere can cause both a huge EMP pulse immediately damaging satellites, radio and radar ground stations, wireless and all manner of other electronic equipment and computers that are in sight of the blast, and that such a device would excite the ionosphere and create radio noise that can last for years, disrupting broadcast signals around the world. Such an attack would require both nuclear weapon and launch capabilities, and hardening of the perpetrator's own equipment against the pulse and after noise.

Adversary Weapons and Tactics

- Space launch and large-scale nuclear weapon capabilities.

- EMP hardening of equipment.
- Fiber optic networks and equipment shielding.
- Many other forms of attack would have to accompany this method because this method is not lethal in itself, and it would initiate war.

GEO-10. CRITICALLY VULNERABLE LOCALITIES

Many cities are extremely vulnerable to natural or intentional disaster. New Orleans is built below sea level and is vulnerable to storms from the Gulf of Mexico and floods from the Mississippi River; the wetlands that protect it from the oceans' waves are disappearing as the land sinks and sea level rises. In addition, New Orleans is surrounded by refineries and oil and gas storage facilities. Houston has similar structures and is barely above sea level, but is somewhat better protected. Venice is at sea level and sinking. Many cities, e.g., Miami, and vacation communities with large numbers of people are located along the Atlantic and Gulf coast and are extremely vulnerable to hurricanes. Seattle is next to Mount Rainier, anticipated to be an active volcano sometime in the future. San Francisco and many other great cities of the world are built among known major earthquake faults. Los Angeles and Oakland have fire vulnerable canyons and hillsides laden with chaparral and eucalyptus. While these vulnerabilities have existed, been known, and have, in fact, led to disasters, such vulnerabilities are not corrected, but instead generally are expanded. New technology for modeling these vulnerabilities, initiating them, and accompanying them with other forms of attack that would assault and confuse the residents and increase the damage and the perception of damage, are becoming available. The use of natural vulnerabilities in connection with a widespread, coordinated national or terrorist attack is possible.

Adversary Weapons and Tactics

- Model the natural vulnerabilities of high density locations.
- Design a large-scale attack of which the triggered vulnerability is one element.

GEO-11. TRIGGERS AND MODIFICATIONS OF GEO SYSTEMS

While there is the impression that many parts of the Earth system are slow to change, many have also exhibited rapid change. Individual glaciers have been observed to surge, sometime creating ice dams that can collapse catastrophically. The overturning circulation of the North Atlantic Ocean that keeps Europe relatively warm in the winter has been observed to change rapidly over a few years. The path of the jet stream can lock into certain patterns, creating prolonged drought or wet spells. In ways not fully understood, small changes in the state or operation of these systems can cause very large changes in climate, weather, temperature, precipitation, and thereby, vegetation, animal and fish populations, degree of pestilences, human health, and agricultural yield, among other vital parameters. The severity of El Nino and the latitude of the jet stream are very influential conditions that significantly affect the weather in the US, and in South and Central America.

Data and knowledge of the physics of these systems is improving due to space, ocean, and land sensor technology, and modern computational models. It is very likely that we will soon come to better understand what triggers the El Nino events, the causal relationships coupling global atmospheric circulation and local weather, and the factors affecting ocean currents and the thermohaline system in particular. Some model simulations calculate that global warming might destabilize the Gulf Stream and bring much colder weather to eastern North America and northern Europe, as it apparently did during the Little Ice Age.

Although very speculative, it is possible, as we learn the relationships between subtle geo system causes and large effects, that event triggers that are energetically and physically achievable will be found. This would offer the potential of using geo systems directly as weapons. It is also very likely that the local weather effects of global climate and circulation will be clear. Unintended, but disadvantageous consequences (drought, desertification, dramatic temperature shifts) might provoke deliberate hostile responses.

The increasing concentrations of greenhouse gases are projected to cause significant global warming and changes in precipitation, causing both adverse and beneficial changes. Generally it is felt that adverse impacts will be much larger for developing countries than for developed countries. This creation of seeming winners and losers, even if only relative, has the potential of creating significant global tensions and stresses. Building the consensus to take actions will be extremely challenging.

Technical fixes, like limiting the warming of the Earth by increasing its albedo (or lofting large satellites to shade the Earth), or changing the ocean's evaporation rate by altering its surface physics, are possible, but are large in scale and cost, and are very likely to have large scale side effects. Such systems are also likely to be quite vulnerable to destruction, which could lead to rapid and possibly destabilizing environmental changes. The chaotic aspects of natural systems might also very well frustrate these intended effects.

In addition to the climatic and geo system state changes, all sorts of secondary effects can occur, from temperature-change-driven species migration and disease emergence, to storm pattern and frequency changes and vegetation shifts with loss of habitats. These in themselves can have major impact on human well being.

We do not know to what extent we can understand the connectedness of geo systems, and moving to control them would require an audacious reach beyond current understanding. Determining whether one would create a benefit, an opportunity for mistake, or a weapon is not at all clear.

Adversary Weapons and Tactics

- Models and globally coordinated data are essential and will give advantage.
- Sense relevant parameters in the depths and heights of the oceans and atmosphere.
- Change the global albedo with aerosols, microspheres, or satellite mirrors.
- Change the ocean surface physics with fluids or films.
- Use seeding or volumetric weapons to trigger and deflect storms.

GEO-12. LAND AND OCEAN FOOD SUPPLY DESTRUCTION

The bio-geo systems that support farming and natural food chains in the oceans, forests, fields, and soil might be destructible, or at least disruptible, and might be the vehicles for intentional attacks on food supplies. In the first instance, some of the disruptions discussed above under natural disasters (GEO-7) and geosystem modification (GEO-11) might be targeted at agricultural assets. Drought, flood, wind, and fire can do widespread damage to crops and livestock. Oceans are being depleted by over-harvesting and damaged by eutrophication and other eco-damaging results of run-off from continental rivers, by waste dumping, and by significant geo system modifications, such as changes in currents, water temperatures, or salinity. Food systems might also be damaged by poisoning the crop or eliminating key species in the food chain, or interaction of harmful genetic modifications.

In addition, biological attacks could be made on food resources, including the introduction of hostile alien species, of sterile or genetically harmful food species variations, of toxins and antigens, or of antibiotics DNA targeted at the keystone food species. Finally, food species might be altered to introduce features that are harmful to animals and humans. While direct application of these weapons would be most efficient, there might be applications which use geo systems for distribution, if the weapon is very potent and a wide distribution needed.

Adversary Weapons and Tactics

- Models for geo systems.
- Models for food cycles and chains.
- Species targeted bio weapons.
- Introduction of harmful alien species.

GEO SYSTEMS TECHNOLOGIES WITH THE GREATEST THREAT POTENTIAL

1. Nuclear Weapons. Nuclear weapons might be used to provide the initiating energy for storms, earthquakes, land slides, tsunamis, or ocean floor slumps or gas releases.

2. Biological Pathogens. Natural pathogens, such as, viruses, bacteria, and fungi, can be transported to new habitats, e.g., the West Nile virus in the US; the atmosphere, wind, and water currents or vectors that live in these systems can be used to distribute pathogens; pathogens introduced into a geo-system or habitat can modify or harm plant and animal species within the new habitat; generally, the large scale of geo systems might transport or widely distribute pathogens or their vectors.

3. Genetic Modifications. Genetically modified plants and animals will change ecological balances and could lead to extinctions of less favored natural species; similarly, the modified species might prove fragile or health hazardous; depending on scale, genetically modified species could produce modified geo-physical effects such as changes in evaporation or albedo.

4. Chemical and Heavy Metal Poisons. Chemical and heavy metal contaminants, much the same as biological pathogens and radioactive contaminants, can be released into geo systems, such as water, soil, and wind, and widely distributed, with the direct impact of harming the inhabitants of that system or its users, or the indirect effects of modifying the contained flora and fauna carrying harm to creatures farther down the food chain.

5. Radioactive Contaminants. Radioactive contamination might be dispersed through geo-systems such as local winds and water, or upper atmospheric winds and rain; such contaminants might also cause harm or mutation to the flora and fauna within the contaminated area; the food products taken from the contaminated area could also be contaminated.

6. Conventional Explosives. Conventional and special purpose explosives can be used for dispersal, penetration, ignition, and structure destruction to unleash energy stored in dam systems, fuel depots, mud and land slides, geologic formations, and possibly even earthquakes.

7. Fire Igniters. Deployable miniature, explosive, or volumetric pyrotechnic devices real-time, delayed, or remote controlled, designed to ignite concentrations of biomass or structures, or to disperse and ignite stored fuel or chemicals.

8. Fuel Storage Facilities. Fuel and chemical storage facilities can contain tens to hundreds to thousands of tons of flammable/explosive material, which if precisely dispersed and ignited could have the blast-equivalent effect of a small nuclear weapon.

9. Atmosphere Modifiers. Green house gases and ozone attackers; light absorbing and reflecting particulate matter; pollution gases and particulate matter; airborne acids.

10. Earth Albedo Modifiers. Molecules, like sulfates; microspheres of glass or other materials with tailored reflective properties, gas filled to stabilize at a selected altitude; reflecting satellites; clouds and aircraft contrails; dust; snow; plants; ocean coating films and life forms.

11. Ocean Surface Modifiers. Films; fertilized algal blooms; non-native flora or fauna.

12. Methane Hydrates and Carbon Dioxide In Deep Waters. Carbon dioxide and methane in the form of hydrates exist in deep waters at equilibrium with the temperature and pressure at depth; occasionally, these deposits are upset by movement by currents to lesser depth and lower pressure, or changes in temperature, say by volcanic action, which destabilize and release these gases into the atmosphere, causing suffocation of inhabitants; upwellings in the ocean are thought to be responsible for mysterious ship disappearances; clathrates in the Gulf of Mexico alone are reputed to contain methane equal to 100,000 times the known global deposits of natural gas; if volatilized and ignited, this could cause catastrophe.

13. Coupled Models Of Geophysical Phenomena At All Scales. Models exist for global climate simulation, for regional weather, for local dispersion, for global ocean currents, and for many large regional and global bio systems; during the next two decades, computational capability and much increased data will enable the coupling of these models such that specific local effects can be related to large-scale or remote changes; it is also possible that triggers will be found which initiate large-scale, extremely high energy geo-system actions, like violent storms and modified precipitation patterns.

ACRONYMS

AIDS	Acquired immune deficiency syndrome
AIP	air independent power system
ASAT	Anti-satellite
ASW	Anti-Submarine Warfare
AVLIS	Atomic vapor laser isotope separation
AWACS	Airborne warning and control system
BNC	Bio-nano-cyber
BTWC	Biological and Toxin Weapons Convention
C4ISR	Command, control, communication, computer, intelligence, surveillance, reconnaissance
CECOM	US Army Communications - Electronics Command
CCPR	Center for Counterproliferation Policy Research - NDU
CGSR	Center for Global Security Research - LLNL
CIA	Central Intelligence Agency
CISAC	Center for International Studies and Cooperation - Stanford University
CISP	Center for Information Strategy and Policy
CLO	Counter low observable
CM	Cruise missile
COMSEC	Communication/computer (network) security
CONUS	Continental United States
COTS	Commercial off the shelf
CTB	Comprehensive Test Ban
CWC	Chemical Weapons Convention
DARPA	Defense Advanced Research Project Agency
DNA	Deoxyribonucleic acid
DOD	Department of Defense
DOE	Department of Energy
DSB	Defense Science Board
DTRA	Defense Threat Reduction Agency
ELF	Extremely low frequency
EMP	Electromagnetic pulse
EO	Electro optical
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GPS	Global Positioning System
HAC	Hughes Aircraft Company
HIV	Human immunodeficiency virus
IAEA	International Atomic Energy Agency
ICBM	Intercontinental ballistic missile
ID	identification
IDA	Institute for Defense Analyses
IIS	Institute for International Studies, Stanford University
IMF	International Monetary Fund
INS	Inertial navigation system
IPSI	International Planning Services, Inc.
IR	Infrared

IRBM	Intermediate range ballistic missile
IRFPA	Infrared focal plane array; an IR imaging sensor
IRST	Infrared search and track
ISO	International Standards organization
ISR	Intelligence, surveillance, reconnaissance
IT	Information technology
LANL	Los Alamos National Laboratory
LEO	Low Earth orbit
LLNL	Lawrence Livermore National Laboratory
ManPAD	Man portable air defense (missile)
MEMS	Micro-electro-mechanical system
MIRV	Multiple independent reentry vehicle
NACO	National Assessment Coordination Office
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NDU	National Defense University
NPT	Nonproliferation Treaty
NRL	Naval Research Laboratory
NSA	National Security Agency
OSD	Office of the Secretary of Defense
SAIC	Science Applications International Corporation
SIGINT	Signal intelligence
SPOT	French satellite Earth imaging system
START	Strategic Arms Reduction Treaty
TRAC	Threat Reduction Advisory Committee
UAV	Unmanned aerial vehicle
UN	United Nations
USAF	Us Air Force
UV	Ultra violet
WTO	World Trade Organization