Preprint
UCRL-JC-141358-REV-1

After Globalization: Future Security in a Technology Rich World

T. J. Gilmartin

This article was submitted to
Erice International Seminars on Planetary Emergencies
Erice, Sicily
August 19-24, 2001

August 17, 2001

U.S. Department of Energy

Lawrence
Livermore
National
Laboratory

AFTER GLOBALIZATION:
FUTURE SECURITY IN A TECHNOLOGY RICH WORLD

Thomas J. Gilmartin
Center for Global Security Research
University of California
Lawrence Livermore National Laboratory
Livermore, California 94550

1. INTRODUCTION

Over the course of the year 2000, five workshops were conducted by the Center for Global Security Research at the Lawrence Livermore National Laboratory on threats to international security 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. The participants included US national leaders and experts from the Department of Energy National Laboratories; the Department of Defense: Army, Navy, Air Force, Office of the Secretary of Defense, Defense Threat Reduction Agency, and Defense Advanced Research Projects Agency; the Department of State, NASA, Congressional technical staff, the intelligence community, universities and university study centers, think tanks, consultants on 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. (See Figure 1.) The threats ranged from local/regional to global, from intentional to unintended to natural, from merely economic to massively destructive, and from individual and group to state actions. We were not concerned in this exercise with defining responses to the threats, although our assessment of each threat's severity included consideration of the ease or difficulty with which it might be executed or countered.

At the concluding review, we brought the various workshops' participants together, added senior participant/reviewers with broad experience and national responsibility, and discussed the workshop findings to determine what is most certain or uncertain, and what might be needed to resolve our uncertainties. This paper summarizes the consenses and important variations of both the reviewers and the participants. The full report is available at: http://cgsr.llnl.gov/global/global.html

2. MAJOR CONCLUSIONS

In all, 45 threats over a wide range of effects and probabilities of occurrence were identified, as were 60 enabling technology categories. Here we present the major conclusions, which each include consideration of several threats and their enabling technologies.

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, but related 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. Such extreme and potentially anonymous terrorism might be viewed as effective by hyper-zealous groups.

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 genetic or habitual traits. 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 relatively simple and difficult to detect, and the knowledge of how to accomplish these ends is widespread. Even though the perpetrator might be the victim of his own attack, the potential for serious, widespread disease outbreak and global disruption is considerable.

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. Diverse asymmetries between these nations and their adversaries often make mutual understandings difficult; 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 nuclear weapons, out of desperation or vengeance, or in a low fatality (EMP or deep target) 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 of nuclear conflicts.

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 now 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 variety of alliances with each other and with the primary nuclear powers. This system is inherently unstable, very nonlinear, and far more difficult to crisis manage, if only because the scenarios are many, the interactors diverse, and the management protocols untried and undefined. This threat ranks high not based on any current tension, but because of the uncertainties and the potential for catastrophe.

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 dynamic equilibrium with their complex environments. In contrast, most of man's biological creations serve specific purposes, such as, the production of medicines and organs for human use, and the improvement of the productivity and performance of domesticated species, even of humans. These improvements will not be ecologically tested; such testing would be extremely complex, if possible at all. In fact, the increasing 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 technologies. To quote one project participant, "It will be a brave new world when man controls evolution and the worlds of carbon and silicon converge."

Spread of Advanced Military Technologies

Stealth, anti-aircraft IR (infrared) and radar counter measures, AWACS (airborne warning and control system), 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 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 better sensors and 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 cruise missiles. Add to this that stealth technology is becoming widely available for aircraft, missiles, and ships, which will require greater standoff and other protections for aircraft carriers and AWACS, and that improved IR systems will increase night operational effectiveness. The result will be a diminishment of current modes of air dominance and forward strike capability, possibly the necessity of advanced forces to "share the night," and the need for a new generation of strike and countermeasure technologies. The global availability of advanced military technology is increasing and heretofore dominant technologies are no longer contained.

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, of earthquake initiation, and of methane release from metastable undersea clathrate formations are all 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 will be 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.

Information Warfare

The number and variety of information operations that might be used against communication, communication-dependent infrastructure systems, and commerce 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 with undoubtedly large financial cost and inconvenience. 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 nations' sovereignty, economy, or military security. With adequate wariness and prudent precautions, financial losses, disinformation, security breaches, system intrusions, and infrastructure attacks should be containable and preventable. In fact, the more complex the planned assault, the more probable its detection and avoidance.

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 the US in conventional conflict. In fact, the effectiveness of advanced military units might be increased by adopting techniques currently regarded as asymmetric (flexibility, adaptability, unpredicability).

But, concentrations of value (people, cities, infrastructure, industry, energy supplies, embassies, ships in port,...) are extremely vulnerable. It is repeated everyday in new reports that free and open societies 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 and new methods for such attacks, and did decry the commonly identified deficiencies of defense measures, it was also agreed that such attacks would not seriously threaten the nations' 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 defenses and emergency responses were all offered as necessary to minimize the dangers from asymmetric threats.

3. GLOBALIZATION

Some of the characteristics of globalization relevant to security are:

Global Markets

Elements of large-scale economies including their needed resources, skills (education) and information, production, distribution, consumption, and finance will be increasingly transnationally organized and valued, and globally interdependent. Francis Fukayama's thesis (The End of History and the Last Man) is that this will lead to greater similarity and cooperation among nations. Clearly this trend diminishes each nation's ability to control its assets, its enterprises, and its people.

Economic Power

The ability to generate and control global markets has replaced military strength as a strategy for and measure of dominance and security, for examples, with Germany and Japan, and the intention of China.

Private Capital; Criminality

The scale of private money holdings is larger than of many nations. More money flows across national borders every day than the size of the US GDP. George Soros was personally able to stimulate a monetary crisis in South Asia, which threatened even China; on the other hand, he personally pours hundreds of millions of dollars into the rehabilitation of eastern European nations. Criminal cartels' money and thereby political control are threats to national survival in, for examples, Columbia and Russia.

Information Ubiquity

The Internet distributes information without regard to national borders, both intentionally for the purposes of collaboration and business, and unintentionally due to imperfect cyber security and malicious actors. With now wireless technology and wideband networks, almost no place on earth is not connected to the pool of human information and knowledge instantaneously. All the genies are out of the bottles.

Interconnectedness; Disinfrastructurization

One interesting aspect of this global interconnectedness is the ability to organize activities without localization and centralization constraints. Production resources are globally distributed, but coordinated as though they were in the same plant, using facilities wherever they are available, greatly increasing economic efficiency, but also enabling distributed production of weapon systems in a manner that eludes detection and control.

Dynamic Socialization; Migration

Countering Fukayama's optimistic view of globalization, Samuel Huntington (The Clash of Civilization's and the Remaking of the World Order) writes that cultural differences will persist and cause conflict as globalization brings us all into closer contact and forces heretofore incompatible values to somehow coalesce. Both the attraction of global action centers and the exposure of relative deprivation will drive migration and the relaxation of extreme social gradients.

Conformed Governance; Standards, Law, Finance, Civil Rights, Environment

Fundamental to economic cooperation are developed and compatible systems of standardization, law, and finance, which enable business. Increasingly, civil rights and environmental standards are being tied into the terms for international transactions. The International Standards Organization, World Trade Organization, International Monetary Fund, and World Bank are examples meta-national organizations that require nations to bend to the global will and values.

Haves and Have-Nots

Food and money once defined the principal distinctions between have and have-not populations. This contrast was most often local and led to conflict or migration. Today and increasingly in the future, the dimensions which divide haves and have-nots include energy resources, nuclear weapons, information technology (the digital divide), and attitudes toward and the possession of genetic technology. Possession of nuclear weapons by some states in a region causes sharply different national stature and national risks. Genetically modified crops have benefited China in many ways, increasing crop yield and decreasing the use of pesticides; China is very supportive of many forms of genetic innovation. France is much more cautious. Both the advantages and problems of these extreme views will accumulate and differentiate among nations, influencing their ability to commingle their people and their economies.

4. NUCLEAR, MISSILE, AND SPACE TECHNOLOGY

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 formidable weapons, the ability to deter superior conventional forces, 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.

The web of nuclear threats is more complex now than it was during the Cold War. (See Figure 2.) The old actors remain; new actors have come on the scene or increased their capability; and the level of nuclear and platform technology has increased in regions of cultural and resource tensions, such as, the Middle East and the Caspian area. 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.

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."

While it is reasonable to hope that the few massively armed nations will respect each others' capabilities and devise agreements and procedures that will continue to lessen, but probably never eliminate, the threat of massive nuclear war, it seems equally likely that nuclear weapons will gradually proliferate as the world becomes increasingly technological and nuclear energy is increasingly needed, and that a regional nuclear event or terrorist action will occur. Needless to say, these three possibilities should motivate extreme international cooperation in the effort to prevent them.

5. MILITARY TECHNOLOGY

The advanced industrial nations can dominate adversaries in symmetric engagements; they have the asymmetric advantage in a "fair fight.," that is, in large scale force on force warfare. But, they 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. The global leaders generally respect each others laws, 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 for advantage against nominally stronger foes.

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 all advanced nations, but the US particularly will have to deal with this kind of "asymmetric warfare'" in the future.

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 asymmetric techniques, the adversaries' advantages and effectiveness might lessen.

Perhaps the greater fear is that our current military advantage will diminish, as improved IR and radar systems diminish the effectiveness of stealth and countermeasures, as improved range, speed, and stealth of anti-aircraft and anti-ship missiles push support systems back from the theater, and as satellite systems improve adversaries' intelligence. In addition, adversaries use of modern 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 underground 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 industrial nations might be less likely to intervene outside of their homelands, and will be more wary in protecting their homes.

6. INFORMATION TECHNOLOGY

Several general observations relevant to the prediction of the future 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 more conventional 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, theft; persuasion, propaganda; and so on.

Finally, cyber crime is still relatively unconstrained and retribution free. The perpetrators act anonymously, from unknown 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, institutions, 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, non-national 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 disrupters.

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 access 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.

The consensus of our discussions, however, was that, while information technology and operations will be extremely important elements of both offense and defense, physical dominance is more likely to determine that outcome of conflicts during the next two decades.

7. BIOTECHNOLOGY

While the participants in the Biotechnology 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. These future (and already emerging) capabilities would both increase the range and lethality of current bio threats, and would enable significant new types of accidental or intended bio threats.

Agricultural genetic modification has been underway for centuries (breeding) and for over a century on the basis of biological science (Mendel). Genetic manipulation 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 health 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, but also 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 global bio 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 within the US 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, longer- and broader-view authorities might be commissioned for ongoing study and guidance of global biological policy, regimes, and R&D programs.

8. GEO SYSTEMS TECHNOLOGY

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, one megaton every 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 consequences of a triggered natural event extremely 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 economies (e.g., the drought, fires and economic collapse of economies in southeast Asia in the latter 1990s) that can have ripple or even tidal effects around the world. The potential to release huge natural energy and cause widespread disruption could 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 local course of evolution. The ability to modify or corrupt these vast eco-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 well informed.

ACKNOWLEDGEMENTS

This project was conceived and sponsored by Ronald Lehman, Director of the Center for Global Security Research, and led by Thomas Gilmartin, a senior fellow at the Center. The Workshop chairs were: William Schneider (Nuclear, Missiles, and Space Technology), Louis Marquet and Walter Sooy (Military Technology), Joseph Markowitz (Information Technology), Charles Cantor (Bio Technology), and Michael MacCracken (Geo Systems). For their service on the Senior Review Panel, we would like to thank George Shultz, Arthur Cebrowski, Jay Davis, Victor Reis, Paul Saffo, Bruce Tarter, Anthony Carrano, Chris Chyba, Jeffrey Cooper, James DeCorpo, Ted Gold, Donald Hicks, Robert Joseph, Steven Kornguth, James Lang, Michael May, John Nuckolls, James Richardson, Wayne Shotts, Richard Wagner, and Lowell Wood. We would like to express special thanks to Paul Saffo, Walt Sooy, Lowell Wood, Leonard Weiss, and Milt Finger for conceptual contributions. Thanks also for the participation of Eileen Vergino, Deputy Director of the Center, and for Karen Kimball's administration of and Tami Alberto's assistance with this project.

Figure 1. Future Security in a Technology Rich World. The array of technologies that are increasingly available globally from a wide range of sources create wealth and give both offensive and defensive power to nations, sub-nationals, and even individuals.

Figure 2. Post-Cold-War Web of Global Nuclear Weapon Threat Relationships. The predominantly bi-polar nuclear weapon stand-off of the Cold War has given way to a set

of multi-polar, interconnected relationships among nations and entities with dissimilar arsenals and technical capabilities, incompatible motivations, and political instabilities.

This work was performed under the auspices of the U.S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under Contract No. W-7405-Eng-48.

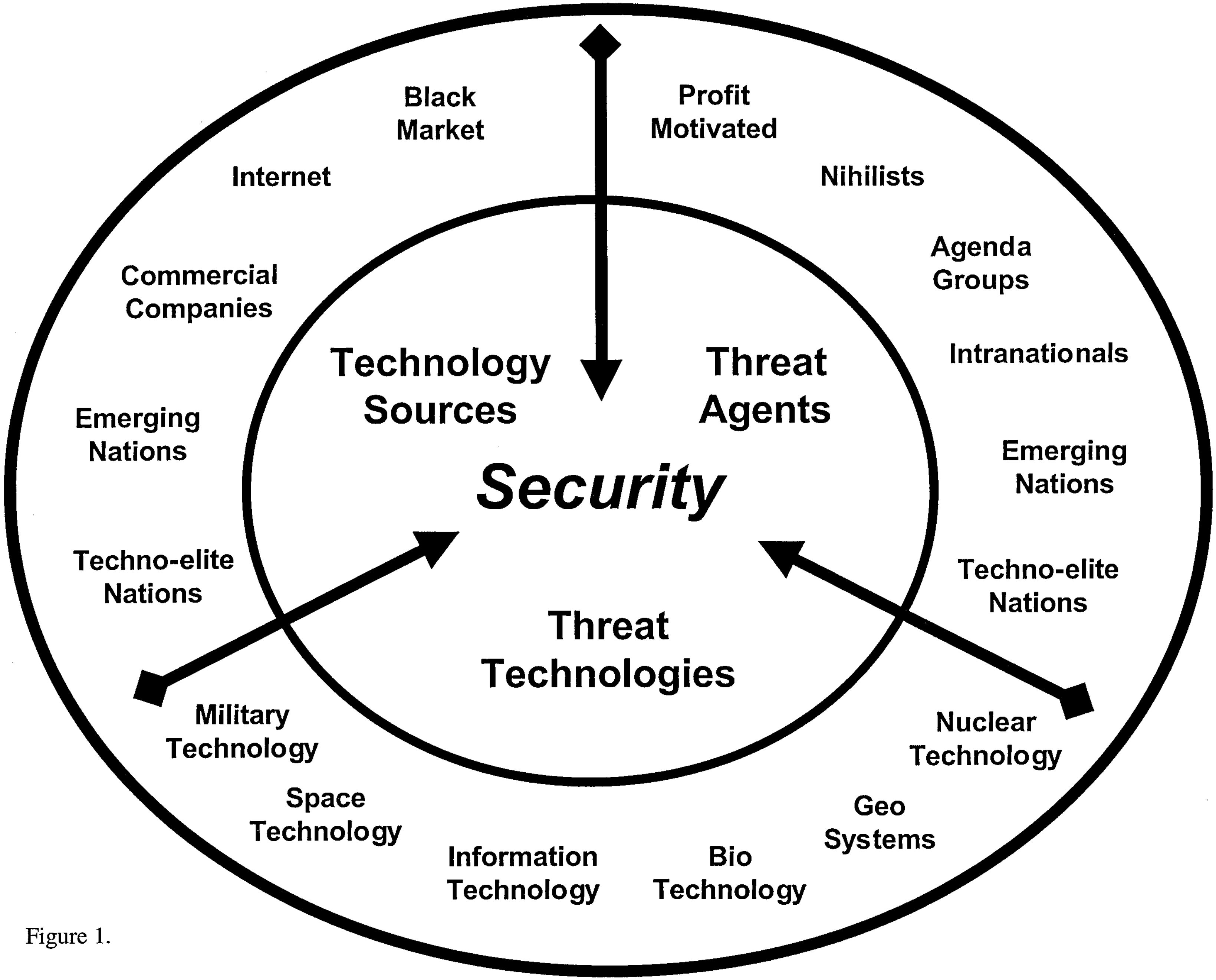
Black
Market
Profit
Motivated
Internet
Nihilists
Agenda
Groups
Commercial
Companies
Intranationals
Technology
Sources
Threat
Agents
Emerging
Nations
Emerging
Nations
Security
Techno-elite
Nations
Techno-elite
Nations
Threat
Technologies
Military
Technology
Nuclear
Technology
Space
Technology
Geo
Systems
Information
Technology
Bio
Technology

Figure 1.

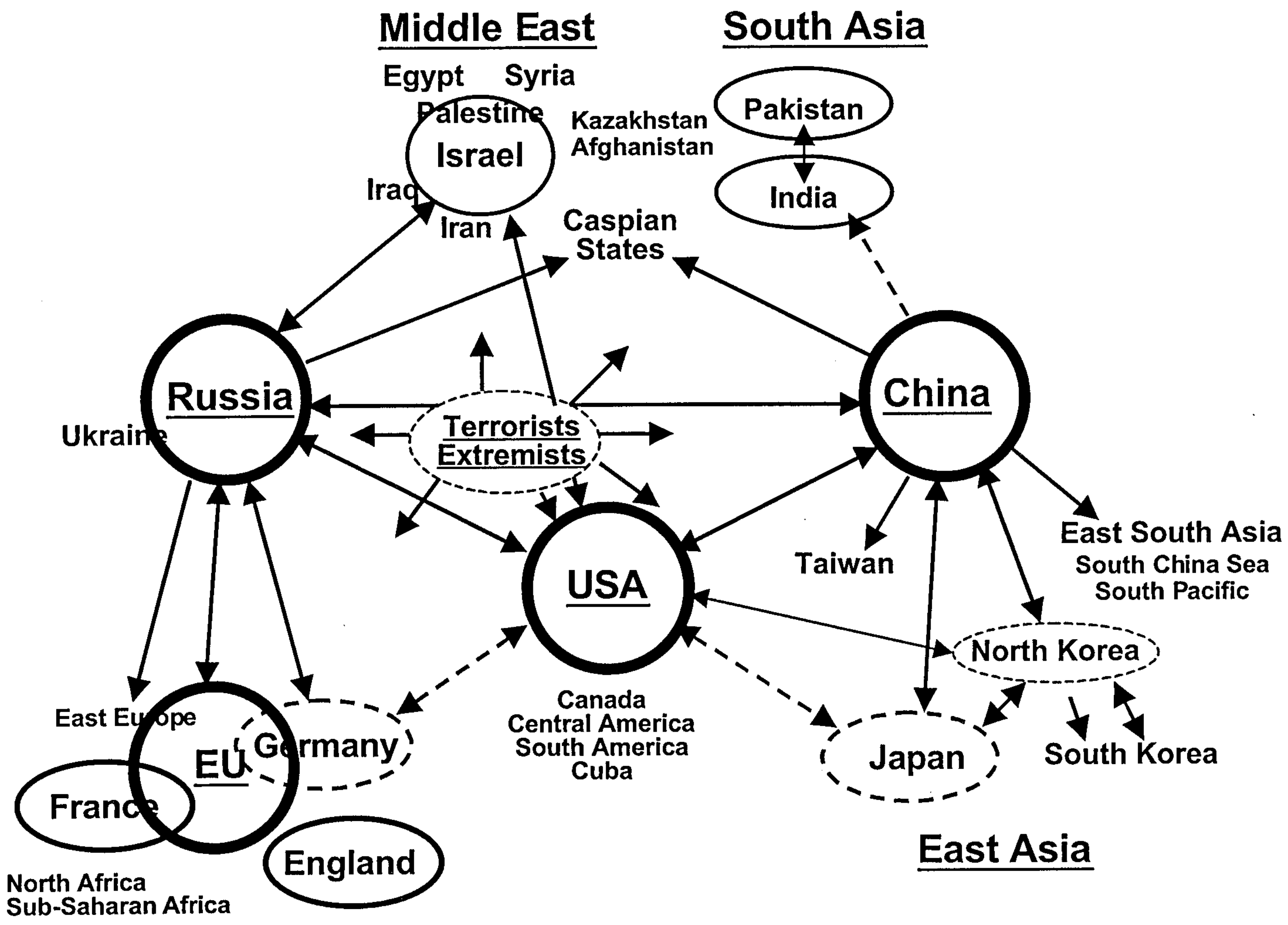
Middle East
Egypt
Syria
Palestine
Israel
Iraq
Iran
Kazakhstan
Afghanistan
South Asia
Pakistan
India
Caspian States
Russia
Ukraine
Terrorists
Extremists
China
USA
Taiwan
East South Asia
South China Sea
South Pacific
North Korea
Japan
South Korea
East Asia
Canada
Central America
South America
Cuba
East Europe
EU
Germany
France
England
North Africa
Sub-Saharan Africa

Figure 2.