

CSIS

Center for Strategic and International Studies

1800 K Street N.W.

Washington, DC 20006

(202) 775-3270

Web: CSIS.ORG

Acordesman@aol.com

**DEFENDING AMERICA
REDEFINING THE CONCEPTUAL BORDERS
OF HOMELAND DEFENSE**

**Asymmetric Warfare versus Counterterrorism:
Rethinking CBRN and CIP Defense and Response**

**Anthony H. Cordesman
Arleigh A. Burke Chair for Strategy**

December, 2000

Table of Contents

ASYMMETRIC WARFARE VS. "TERRORISM"	3
Asymmetric State or Efficient Terrorist Attacks versus the Conventional Picture of "Terrorism"	4
The Problem of Probability	5
The "Theater" Aspects of Asymmetric Warfare and Homeland Defense	6
Do Asymmetric and Terrorist Attack Have Important Elements in Common?	8
Do Asymmetric and Terrorist Attack Differ in Important Elements?	9
ASYMMETRIC WARFARE: RECONSIDERING OFFENSE, DEFENSE, AND RESPONSE	10
Federal Government Does Not Currently Respond Effectively to the Threat of Large-Scale and Asymmetric Attacks	11
Asymmetric Warfare: Finding Solutions	12
Reconsidering the Sophistication and Level of Attack	13
The Need for an Unambiguous Strategic Offensive Doctrine	14
Asymmetric Warfare: Offensive Defense	15
Asymmetric Warfare: Intelligence, Threat Assessment, Offense, Defense, and Response	17
Asymmetric Warfare: Defensive Defense	18
Asymmetric Warfare: Net Technical Assessment	19
Asymmetric Warfare: Attack Characterization is Critical to Defense and Response	20
Asymmetric Warfare: Decentralized and Distributed Response	21
Asymmetric Warfare: Rethinking Civil Defense	22
ASYMMETRIC NUCLEAR WARFARE VS. NUCLEAR TERRORISM	23
Asymmetric Warfare: Unthinking the Thinkable About Nuclear Attacks - I	24
Asymmetric Warfare: Unthinking the Thinkable About Nuclear Attacks - II	25
Asymmetric Warfare: How Can Technology Deal with The Nuclear Risk?	26
ASYMMETRIC BIOWARFARE VS. BIOTERRORISM	27
Unthinking the Thinkable About Asymmetric Biological Warfare - I	28
Unthinking the Thinkable About Asymmetric Biological Warfare - II	29
Asymmetric Warfare: Militarized and Infectious Biological Attacks	30
Asymmetric Warfare: Advances in Biological Weapons - I	31
Asymmetric Warfare: Advances in Biological Weapons - II	32
Asymmetric Warfare: How Can Biotechnology Deal with This Risk?	33
Asymmetric Warfare: Implications for Public Health Services and Hospitals	34
Asymmetric Warfare: Must Also Deal with Agricultural and Ecological Warfare	35
CYBERWARFARE VS. CYBERTERRORISM	36
Asymmetric Warfare: What Does Cyberwar Really Mean?	37
Asymmetric Warfare and Attacks on CIP/Information Systems	38
Asymmetric Warfare and CIP/Information Systems: Is There an Offensive Option?	39
CIP/Information Systems: the Need for Degenerative, Non-Vulnerable, and Replacable Systems	40
Asymmetric Warfare: Timelines and Responsibility	42

ASYMMETRIC WARFARE VS. “TERRORISM”

*Asymmetric State or Efficient Terrorist Attacks versus the Conventional Picture of
“Terrorism”*

- **Threats involve different levels of sophistication and intensity, and probably very different methods of attack and technologies.**
- **The problems of warning, defense and response differ sharply by level of attack and threat.**
- **The rules change for all responders as attacks escalate from conventional low-level terrorism (“crooks and crazies”) to major levels of damage and casualties:**
 - **National emergency forces DoD into critical role.**
 - **Law enforcement must operate in state of national emergency. Issue of state of war becomes real prospect.**
 - **Public health and emergency services saturated and face reality can only half-anticipate.**
 - **Possible threats to basic structure of commerce, economic infrastructure, continuity of government.**
 - **May well be linked to a serious theater-driven crisis or war.**

The Problem of Probability

- **Low level terrorist attacks are indeed more probable, and in fact are constantly occurring at the cyber and false alarm level.**
- **Seen over a 25 year period, however, the probability of some sophisticated form of major asymmetric attack is high.**
 - **Not only on US, but our allies.**
- **We have a “Non-Gaussian” reality. There is no standard distribution curve.**
- **The cumulative probability over time of a low to moderate probability event actually be the highest priority for planning is much higher than the probability the most probable events will actually be the highest priority for planning.**
- **We cannot deal with the problem by adding analytic and technological elegance to the classic American solution to all critical problems: “Simple, quick, and wrong.”**

The “Theater” Aspects of Asymmetric Warfare and Homeland Defense

- **Threat is not directed at US per se, but at US as extension of regional/theater/foreign nation objectives.**
- **Allied targets, US forces and businesses overseas, and critical economic facilities can be targeted, not just US.**
- **Multiple and sequential attacks more likely, as are mixes of methods of attack.**
- **Availability of sophisticated biological and nuclear weapons more likely.**
- **CIP offers a low cost adjunct to virtually all forms of asymmetric and theater warfare.**
- **Crisis/war driven intentions and escalation extremely difficult to predict.**
 - **History is irrational and is often made out of worst cases. Intelligent, prudent, “business as usual” intentions usually means crisis never occurs in the first place.**
 - **Asymmetric values and perceptions are as real as asymmetric warfare.**

Do Asymmetric and Terrorist Attack Have Important Elements in Common?

- **All threats relate to other national security activities.**
- **All compete for limited resources and federal emergency management capabilities.**
- **“Squeezing the balloon:” Defending in one area while failing in the others pushes attackers to attack the less defended area.**
- **Many common problems in law enforcement.**
- **Many common problems in public health and emergency services.**
- **All depend on the relative vulnerability of commerce, economic infrastructure, continuity of government.**
- **All create the risks of attacks with effects so costly that response may prove unaffordable, and where it is unclear that technology and systems are available for effective response.**

Do Asymmetric and Terrorist Attack Differ in Important Elements?

- **Natural difference in priority between Defense and Law Enforcement/Responder communities. Each focuses on business as usual.**
 - **Responders/defenders do not focus on “mission impossible.”**
 - **Linkage to foreign threats and wars largely ignored outside the Department of Defense and national security community.**
- **Intelligence and law enforcement efforts decoupled. Serious legal barriers to effective action.**
- **Asymmetric warfare can push US rapidly towards Presidential state of emergency, most terrorism is business as usual.**
 - **Defense/response has priority over normal legal procedures and civil rights.**
 - **Breakdown/collapse of local defense and response efforts is a much higher priority.**
- **Risks of attacks with effects so costly that response may prove unaffordable is much higher, as is uncertainty that technology and systems are available for effective response.**
 - **If cannot defend, must respond as well as retaliate.**

ASYMMETRIC WARFARE: RECONSIDERING OFFENSE, DEFENSE, AND RESPONSE

Federal Government Does Not Currently Respond Effectively to the Threat of Large-Scale and Asymmetric Attacks

- **Really have not conducted systematic threat evaluation of who can really use different kinds of CBRN weapons and methods of attack, and how technology will evolve over next 25 years .**
- **Legalistic approach prevents effective action. Much of law and human rights discussion fails to distinguish between the need to respond differently to a critical attack/existential threat and a lower level incident.**
- **Failure to integrate theater and homeland offensive/defense issues.**
- **“C,” “B,” “R,” and “N” threats and poorly defined. Warning, intelligence, defense, and response tend to be compartmented.**
- **Effects models dubious at best and unsuited for response planning.**
- **Failure to realistically address major nuclear and biological attacks, examine limits of what response can and cannot do.**
- **Defense and response programs tend to be compartmented. Create open-ended programs with no clear picture of what deployed system will look like and cost.**
- **Major problems in biological side with proposed solutions decoupled from massive public health cost problems and reduction in hospital and emergency care capabilities for cost-effectiveness reasons.**
- **Lack of Net Technical Assessment and realistic evaluation of cost to defeat proposed programs and solutions.**
- **Failure to explicitly consider offensive and retaliatory options against foreign attack.**

Asymmetric Warfare: Finding Solutions

- **Re-evaluate the threat in terms of warfighting and not just “terrorism.”**
- **Force common intelligence/defense/response planning for high level “C,” “B,” “R,” and “N” attacks.**
- **Re-examine theater and homeland offensive/defense issues: Consider post Cold-War strategic and theater offensive/retaliatory options, including nuclear.**
- **Look honestly at the critical threshold where existing federal, state, and local response options fail: The nuclear and critical biological attack.**
- **Examine the real-world limits of intelligence, warning, and defense.**
- **Create a “zero-based” review of the real-world impact of CBRN weapons on critical targets and urban environments. Look at the reactor problem.**
- **Require Net Technical Assessment and realistic evaluation of “cost-to0defeat” proposed programs and solutions.**
- **Conduct a “zero-based” review of legislation to clearly define how intelligence and law enforcement can be made more effective, and the trade-offs involved.**
- **Treat CBRN response in the full context of national public health requirements. Determine what is really practical and affordable.**
- **Create an effective program budget, not simply an annual budget.**
- **Evolve the right solution to real problems.**

Reconsidering the Sophistication and Level of Attack

- **All attacks are not created equal. Limited CBR attacks at the terrorist and extremist level are fundamentally different from nuclear and highly lethal nuclear and biological attacks.**
 - **Covert and proxy attacks by foreign governments are acts of war. Truly sophisticated terrorists will not operate under the limits currently assumed in most studies.**
 - **Such attacks sharply raise the probability of “cocktails” of different agents, mixes of CBRN and cyber attacks, and the use of such attacks to supplement theater conflicts. NMD + CBRN + CIP is then credible.**
 - **The current and perhaps any affordable response effort will collapse at finite and limited levels, forcing federal/state/local governments and the private sector to improvise radically.**
 - **Bioattacks with immune or genetically engineered strains that have unpredictable delays, persistence, symptoms, ability to defeat treatment and vaccines, and lethality become a real possibility.**
- **The “balloon effect” means that attacker will respond to US defensive measures by (a) shifting their methods of attack to strike at the least defended areas, and (b) developing countermeasures to exploit the weaknesses in any defense.**
 - **This makes “cost to defeat” and net technical assessment of all defensive programs and options critical.**
- **There does not seem to be any current prospect of dramatic changes in the ability to build a nuclear bomb in the basement and in domestic/foreign terrorist ability to acquire nuclear weapons.**
- **The situation with biological technology *may* be radically different. Bioattacks with immune or genetically engineered strains that have unpredictable delays, persistence, symptoms, ability to defeat treatment and vaccines, and lethality then become a real possibility.**

The Need for an Unambiguous Strategic Offensive Doctrine

- **We are drifting towards a response-oriented approach that does not even have a Maginot Line-like emphasis on defense.**
- **Major attacks must be firmly deterred, preempted or reduced in size, and firmly retaliated to.**
- **It must be clear that attacking states, and states that deliberately host terrorist movements, will be the target of US strikes directed at the nation and not simply at the leadership.**
- **The US needs to give its theater and strategic forces this option.**

Asymmetric Warfare: Offensive Defense

- **What changes to deterrence, offensive strike capability, and retaliation really matter if states and foreign movements are involved?**
- *What can be done to aid defenders in securing US borders and territory?*
- *What can be done in terms of intelligence/technology to rapidly and conclusively identify the attacker?*
- **What can be done to accelerate and improve warning time for offensive/counterattack/deterrent purposes?**
- **When is the threat/attack one that justifies “war?” When is “legalism” over?**
- **What should the retaliatory doctrine be?**
 - **How lethal should the escalatory action be?**
 - **Halt or punish the attacker?**
 - **Prevent follow on attacks? Deter future attackers?**
- **Homeland/theater linkage. What acts to:**
 - **Enhance force protection?**
 - **Protect allies?**
 - **Deter third party adventures and copycats?**

- **Cope with multiple, mixed (cocktail), and sequential attacks.**

Asymmetric Warfare: Intelligence, Threat Assessment, Offense, Defense, and Response

- **When is the threat/attack one that justifies decisive defensive action? When does a true state of emergency begin and when is “legalism” over?**
- **Establishing opportunities and limits for intelligence capability is critical to effective action.**
- **How much can targeting, precision strike, weapons effects, and BDA really be improved?**
- **Limiting asymmetric capability and peacetime improvements in threat characterization are critical: Limiting and monitoring technology transfer and RDT&E efforts is the first line of defense.**
 - **Nunn-Lugar is extremely cost-effective Homeland defense. Needs to be fully extended to biological weapons.**
 - **Sanctions and supply regimes are highly effective tools. Supplier and shipper monitoring, literature and media “mining,” “flares” in political statements.**
- **What can be done to improve or replace HUMINT? Can data-mining and AI provide a new technological approach?**
 - **The myth that expanding HUMINT efforts will help either needs to be transformed into a reality or dismissed.**
 - **How can cooperation with our allies intelligence services and international law enforcement agencies be used as a first line of defense?**
- **Detection of effort to proliferate is not enough. Need to characterize the nature of possible attacks as precisely as possible to reduce burden on defender and responder, and help prioritize and define options for offensive/counteroffensive action.**
 - **Nuclear weapon type and yield. (Accuracy/HOB)**
 - **Special biological agents, strains, capacity to genetically engineer, delivery options, dry/storable?**
 - **Probable number, sequence, and mix of attacks.**

Asymmetric Warfare: Defensive Defense

- **Does new technology and a systems approach really offer any significant statistical/actuarial help to the defender in detecting CBRN attacks in ways that allow a defensive response?**
 - **Is improved border coverage possible and cost-effective? Only NR or CB as well? National or localized, emergency capability with warning?**
 - **21st Century NEST: If you zero-base the concept, can you really do more to protect borders or find the weapon? If you have an attack, can you improve the search for additional weapons?**
 - **Is there any credible form of “Bio-NEST”? Is there any hope of search technology to find biological (chemical) weapons?**
 - **Is any kind of distributed detection and diagnostic system technically credible and cost effective? What operational research is needed into search and detection options**
- **What can be done to give defenders rapid capability to secure/sterilize/decontaminate an area with suspected CBRN weapons with minimum collateral damage?**
- **When is the threat/attack one that justifies decisive defensive action? When does a true state of emergency begin and when is “legalism” over?**

Asymmetric Warfare: Net Technical Assessment

- **GIGO: Critical effectiveness and lethality data are very uncertain and modeling is becoming more sophisticated rather than more accurate.**
- **Attack models are weak, and cannot be rapidly tailored to simulate specific types of attacks on specific cites and targets.**
- **Technology and effectiveness of different means of attack and defense are poorly assessed. Assumptions about the effectiveness of weaponization and delivery methods often have weak technical and empirical rationale.**
- **Lack of Net Technical Assessment means that we are selling and buying too many ideas with:**
 - **Uncertain analysis of probable trends in related defensive and offensive technology.**
 - **No clear technology base for overall prioritization.**
 - **Little or no assessment of the cost to by pass or defeat a given program.**
 - **No assessment of the “end state” in terms of a description of a deployed system and capability and is procurement and life-cycle cost?**
 - **Parochial cost/time/effectiveness models designed to sell the program.**

Asymmetric Warfare: Attack Characterization is Critical to Defense and Response

- **Defensive concepts are now generally stovepiped and oriented to a single attack by one type of weapon. There are no rules that say we do not face multiple or sequential attacks by mixes of weapons.**
 - **If national specialized intelligence, counterterrorism, and law enforcement assets cannot handle this burden, the vulnerability is obvious.**
- **Today's ability to assess the impact of given types of weapons, simulate their actual use in real-world urban environments, and discuss uses of mixes of weapons is based on tenuous and inadequate models that may do more to misinform responders and waste resources than help.**
- **The cheapest way to reduce the burden on local (and federal and state) responders may be to provide the most accurate possible picture of what an attack can do and what response is really required. Since the burden will still fall largely on local responders, intergovernmental coordination and organization is not the key priority.**
 - **There is no point in developing individual types of high technology detectors that cannot be used in effective C,B, R & N systems that can characterize the nature of the attack, the area of the attack, and identify the proper response.**
 - **At the same time, the cheapest way to make the response effort efficient and reduce the response burden would be distributed or rapidly deployable tools that would provide this information and monitor developments like plumes and fall out.**

Asymmetric Warfare: Decentralized and Distributed Response

- **Response needs rethinking to consider truly large-scale and/or multiple attacks.**
- **Most federal and a great deal of state and regional response may come too late to fit the critical time windows for biotreatment. And dealing with the prompt effects of nuclear explosions and fall out.**
- **Some form of decentralized and distributed local/civil defense may be the only answer. The questions then become prompt attack characterization, instructions to flee or stay, proper guidance to responders, and options for very low-cost distributed defensive aids like masks, medicines, etc.**
- **The key limiting factor in terms of capability and expense will be medical treatment. Is any kind of distributed system technically credible and cost effective?**
 - **The issue of *live or let die triage* must be addressed now to guide local responders and determine whether new diagnostic and detection technology can reduce the medical burden.**
- **It is far from clear that response training today really prepares anyone for anything other than relatively small and easily characterized events.**
- **Much of the non-medical response effort seems to be focused around obtaining equipment and facilities to “get well” from past underfunding or provide equipment for small events. It is unclear that creating standard packages of such equipment, or responding to responder’s priorities, really deals with the problem of homeland defense.**
 - **Fixing the firehouse is pork, not homeland defense.**
 - **The question is what kinds of training and equipment really help.**

Asymmetric Warfare: Rethinking Civil Defense

- **Many cheap solutions do exist.**
- **Cannot suboptimize on C, B, R, or N.**
- *Must look beyond asymmetric warfare and terrorism, consider broader national public health priorities, and NMD “leakage” problems.*
- **Real-time warning, characterization, and guidance can cover widest area most cheaply:**
 - **Use of media?**
 - **Flee or stay advice. Detailed in the office, home, and car advice.**
 - **Real time linkage between responder and media.**
- **Credible and affordable low cost options:**
 - **What can citizens, corporations, local, state, and federal governments really afford.**
 - **Masks, tape, home detectors, etc. If cost is low enough, make purchase voluntary.**
- **Ecological and agricultural civil defense?**

ASYMMETRIC NUCLEAR WARFARE VS. NUCLEAR TERRORISM

Asymmetric Warfare: Unthinking the Thinkable About Nuclear Attacks - I

- **There are no reliable models of nuclear weapons effects in major urban areas involving massive complexes of high rise steel and glass buildings. The containment effects of modern cities are extremely difficult to model. Military studies indicate, for example, that modern buildings can reduce the effect of blast, thermal, and radiation by 40-60%, but they do not specifically address modern heating and air conditioning systems, and the sheltering effects are not designed to take glass into account and the internal impact on the building.ⁱ**
- **Nuclear explosions create a wide range of different effects that can interact on the human body. The recent literature on military models for predicting casualties indicates that such models are not reliable, and states that, “The US Army Office of the Surgeon General is developing a system of casualty estimation that will provide rapid and reasonably accurate estimates of the number of types of casualties produced by a given enemy nuclear attack.” This system, however, is not yet available.ⁱⁱ The military handbook on the subject acknowledges that medical facilities will probably be saturated or collapse in the event of a major attack, but effectively dodges the problem of diagnosis and triage, and assumes that adequate medical professionals and facilities are available to allow extended triage and preventive medical treatment.ⁱⁱⁱ The Defense Threat Reduction Agency (DTRA) is working on more sophisticated models tailored to attacks on the US but it again is unclear when any unclassified results will be available.**
- **The impact of prompt radiation is extremely difficult to estimate, and lethal and serious does can vary sharply according to exposure even in the same areas. Even personnel equipped with dosimeters present major problems in triage because dosimeter readings cannot be used to judge whole body radiation, and a mix of physical symptoms have to be used to judge the seriousness of exposure. The impact of radiation poisoning also changes sharply if the body has experienced burns or physical trauma.^{iv} In the case of treatable patients, significant medical treatment may be required for more than two months after exposure.**
- **Fall out can vary sharply according to the size and nature of a weapon and its placement, and in the size and lethality of particles and water vapor. While most fall out settles within 24 hours, this varies according to wind pattern and movement through the affected area. The drop in actual radiation of the affected material is much slower, but logarithmic. Radiation at the first hour after the explosion is down about 90%, and radiation is only about one percent of the original level after two days. Radiation only drops to trace levels, however, after 300 hours.^v**

Asymmetric Warfare: Unthinking the Thinkable About Nuclear Attacks - II

- **The test data on the longer-term (after 24 hours) effects of radiation are highly uncertain and the longer term impacts of radiation are so speculative as to be impossible to estimate. As a result, virtually all estimates of the impact of nuclear weapons ignore the long-term casualties (96 hours to 70+ years) caused by radiation, such as cancer, and the impact of a weapon on the environment in terms of the poisoning of water and food supplies. The data on treatment of exposures from zero to 530 cGy of exposure do not even seem to call for recording the probable level of exposure.^{vi}**
- **There is little data on the steadily growing seriousness of EMP on urban areas filled with computers and solid-state communications and control devices.^{vii}**
- **Most models of fall out assume relatively neat patterns of distribution or plumes that give state and local responders a relatively clear picture of probable lethality and casualty effects. It is uncertain how realistic these models really are. Weather patterns could produce far more erratic patterns of distribution, and some estimates indicate that the “worst case” area covered by the overall plume could easily be twice the area used as the reference case. There is little detailed or parametric modeling of these uncertainties, and of the burden they place on response teams. These uncertainties also are much greater for the much larger areas covered by low levels of radiation over time.**
- **The problem is further complicated by trying to estimate the specific mix of radioisotopes and radionuclides that will be produced and then become induced in the soil. The hazard prediction models used by the Department of Defense are under review, and it is not clear when new models will be available.^{viii}**
- **There is often a gap between generic data on radiation, burn, and physical effects and the assumed level of treatment required. Much of the federal, state, and local response literature effectively dodges around the issue of triage, and the problem of choosing who will receive limited medical treatment and how these victims will be selected. It does not describe what is done with the assumed dying and untreatable. The broader issue, however, is what indicators will be used for triage and deciding treatment and what treatment should actually be employed.**
- **Food and water contamination can be a serious problem, and add to the response burden in any major attack.^{ix} Fallout presents special problems since sheltered civilians may not have access to safe water, and urban water systems may be affected.**
- **Corpse disposal may be a major problem as may disposal of dead animals and birds. This aspect of response seems to be largely ignored.**
- **Even military medical handbooks fail to address the psychological impacts of prompt and longer-term effects.**

Asymmetric Warfare: How Can Technology Deal with The Nuclear Risk?

- **Improved modeling of real-world urban effects. Modeling of fallout and “rain out” plumes in ways tailored to improve response planning.**
- **Near real time fallout corridor modeling and data mining. Modeling for needed level of state, regional, and federal response.**
- **Detection and diagnostic systems – either distributed or rapidly deployable. (e.g. the public transportation sensor grid).**
- **Monitoring of actual distribution of fallout and weapons effects to give local responders a more precise picture of short and long term response requirements. Real-time transmission to responders, and state, regional, and federal actors. (Often 12-48 hour time window for critical response actions).**
- **Systems for instant detection and diagnostics, guidance for response and triage. Dosimeters are useless for this purpose. Need clearly defined stay or flee guidance.**
- **Cheap portable systems for real-time triage analysis.**
- **Improved detection and characterization of residual threats, decontamination technologies and decon effectiveness measuring systems.**
- **Hospital technology solutions, rapidly deployable care technology.**
- **Cheap, simple civil defense options: Masks, no cost what to do technology and advice, media warning and advice alert systems.**

ASYMMETRIC BIOWARFARE VS. BIOTERRORISM

Unthinking the Thinkable About Asymmetric Biological Warfare - I

- **It may not be possible to detect and characterize a biological attack (or attacks) until it is too late to provide effective treatment, to determine what levels of medical resources are required, or know how many response and treatment capabilities have been attacked and what level of patient flow will result.**
- **Much of the current response planning tacitly assumes that either incidents will be small and familiar enough to allow existing response capabilities to work or that attacks will be detected and characterized in ways that allow effective response planning. CDC/USAMIRID, etc. are sized at this level.**
- **Attacks by multiple agents, sequential attacks, attacks designed to create national infectious disease patterns, and mixing these attacks with CIP and cyber attacks is an unthinkable worst case, particularly at the law enforcement and responder level.**
- **Much of the response planning assumes that it is possible to predict the required medical treatment based on limited experience with civil incidents and epidemics. It is not clear that the “scaling” involved in estimating the effect of terrorist, extremist or covert use of more sophisticated weapons is more than speculative, and many studies do not cite the special evidence and method used to scale up civil cases into estimates of how biological weapons would behave.**
- **The uncertainty created by the ability to modify or engineer new weapons or forms of existing weapons greatly compounds these problems. There do not seem to be net assessments of the balance between changes in offensive and defensive biotechnology that allow the US to predict future lethalties or the effectiveness of many proposed response measures.**
- **Most of the measures the US takes to provide homeland defense against biological weapons immediately become part of the open literature, and many take years of lead-time to become effective. While this can act as a deterrent, it can also act as a road map for states and sophisticated extremists in finding the weaknesses in US defenses.**
- **There are a number of detailed problems in detection, characteristics, and effects analysis. For example, reliable models of biological weapons effects do not seem to exist which cover attacks in major urban areas involving massive complexes of high rise steel and glass buildings. The containment and transmission effects of modern cities are extremely difficult to model.**
- **Most effects estimates only apply to the use of one biological weapon, but attacks using “cocktails” of several biological weapons were found to be the most effective method of mass attack during the Cold War.**

Unthinking the Thinkable About Asymmetric Biological Warfare - II

- **There is often a gap between generic data on the treatment needed for a given biological weapon and the assumed level of treatment required.**
- **There is the tacit or explicit assumption that a weapon can be treated as a conventional disease, and that enough will be known about effects and exposure for treatment to be applied.**
- **Much of the federal, state, and local response literature effectively dodges around the issue of triage, and the problem of choosing who will receive limited medical treatment and how these victims will be selected.**
- **Corpse disposal may be a major problem, as may disposal of dead animals and birds. This aspect of response seems to be ignored.**
- **Even military medical handbooks fail to properly address the psychological impacts of prompt and longer-term effects.**
- **Little or no practical planning to deal with longer-term physiological effects and mass decontamination and recovery problems.**

Asymmetric Warfare: Militarized and Infectious Biological Attacks

- **Much of the present approach seems to assume that biological attacks will be limited to non-contagious agents or “crooks and crazies”.**
- **Other work assumes that it will follow containable patterns of normal disease outbreaks.**
- **The use of militarized and genetically modified strains needs explicit analysis.**
- **There seems to be a major decoupling of defensive and response planning from any net technical assessment of the advances taking place in biological weapons.**

Asymmetric Warfare: Advances in Biological Weapons - I

- *Safer handling and deployment*, including the elimination of risks from accidents or misuse – the "boomerang effect".
- *Easier propagation and/or distribution* eliminating the need for a normally-hydrated bioagent or any use of aerosols. Microorganisms with enhanced aerosol and environmental stability.
- *Improved ability to target the host*, including the possible targeting of specific races or ethnic groups with given genetic characteristics.
- *Greater transmissivity and infectivity*: Engineering a disease like Ebola to be as communicable as measles. Microorganisms resistant to antibiotics, standard vaccines, and therapeutics.
- *New weapons*: Benign microorganisms, genetically altered to produce a toxin, venom, or bioregulator.
- *Increased problems in detection*: Immunologically altered microorganisms able to defeat standard identification, detection, and diagnostic methods. Problems in diagnosis, false diagnosis, lack of detection by existing detectors, long latency, binary initiation.
- *Greater toxicity, more difficult to treat*: Very high morbidity or mortality, resistant to known antibacterial or antiviral agents; defeats existing vaccines; produces symptoms designed to saturate available specialized medical treatment facilities.
- *Combinations of some or all of the above.*

Asymmetric Warfare: Advances in Biological Weapons - II

- ***Binary biological weapons*** that use two safe to handle elements that can be assembled before use. This could be a virus and helper virus like Hepatitis D or a bacterial virulence plasmid like E. coli, plague, anthrax, and dysentery.
- ***Designer genes and life forms***, which could include synthetic genes and gene networks, synthetic viruses, and synthetic organisms. These weapons include DNA shuffling, synthetic forms of the flu – which killed more people in 1918 than died in all of World War I and which still kills about 30,000 Americans a year – and synthetic microorganisms.
- ***"Gene therapy" weapons*** that use transforming viruses or similar DNA vectors carrying Trojan horse genes (retrovirus, adenovirus, poxvirus, HSV-1). Such weapons can produce single individual (somatic cell) or inheritable (germline) changes. It can also remove immunities and wound healing capabilities.
- ***Stealth viruses*** can be transforming or conditionally inducible. They exploit the fact that humans normally carry a substantial viral load, and examples are the herpesvirus, cytomegalovirus, Epstein-Barr, and SV40 contamination which are normally dormant or limited in infect but can be transformed into far more lethal diseases. They can be introduced over years and then used to blackmail a population.
- ***Host-swapping diseases***: Viral parasites normally have narrow host ranges and develop an evolutionary equilibrium with their hosts. Disruption of this equilibrium normally produces no results, but it can be extremely lethal. Natural examples include AIDS, hantavirus, Marburg, and Ebola. Tailoring the disruption for attack purposes can produce weapons that are extremely lethal and for which there is no treatment. A tailored disease like AIDS could combine serious initial lethality with crippling long-term effects lasting decades.
- ***Designer diseases*** involve using molecular biology to create the disease first and then constructing a pathogen to produce it. It could eliminate immunity, target normally dormant genes, or instruct cells to commit suicide. Apoptosis is programmed cell death, and specific apoptosis can be used to kill any mix of cells.

Asymmetric Warfare: How Can Biotechnology Deal with This Risk?

- **Detection and diagnostic systems – either distributed or rapidly deployable. (e.g. the public transportation sensor grid).**
- **Systems for instant detection and diagnostics, guidance for response and triage.**
- **Cheap portable systems for real-time triage analysis.**
- **Near real time infection corridor modeling and data mining. Containment modeling. Modeling for needed level of state, regional, and federal response.**
- **Finding the cure: Multivalent vaccines, replicon vaccines, broad spectrum antibiotics, immune system boosters, new antivirals. (*Now being oversold. Needs much more challenging peer group review of project proposals.*)**
- **Improved detection and characterization of residual threats, decontamination technologies and decon effectiveness measuring systems.**
- **Hospital technology solutions, rapidly deployable care technology.**
- **Cheap, simple civil defense options: Masks, no cost what to do technology and advice, media warning and advice alert systems.**

Asymmetric Warfare: Implications for Public Health Services and Hospitals

- **Vague, generalized recommendations to strengthen public health systems, hospitals, and private care must be rethought. Tend to focus on low to mid level B and C attacks, not major BRN attacks.**
 - **Symbolic and half-measures may simply increase cost with marginal increases in capability.**
 - **The present emphasis on vaccines, respirators, and more specialized public health and treatment facilities threatens to be purposeless in terms of cost to defeat, cost to procure, dual-use, value and real world distribution times.**
 - **The actuarial chance a given apparently low cost-fix may actually be required on a national level can be extremely low and the cumulative cost can be extremely high.**
 - **The nation has many ongoing day-to-day health priorities that will increase as the population ages.**
 - **In most large-scale events the real world answer is that effective response in terms of major medical facilities is neither predictable enough to provide or afford.**
- ***But, there may be low-cost distributed health measures that can reduce casualties.***
 - *Note that improving triage and (a) avoiding treatment of those who do not need it, (b) delaying treatment for those not needing urgent treatment, and (c) letting the “walking dead” die may ultimately be the only way to do this.*
 - *Current warning and detection technology is not designed to support this kind of triage, and often will not support effective diagnostics.*
 - *Improved diagnostics is the second area where efficiency seems improvable at the least cost.*

Asymmetric Warfare: Must Also Deal with Agricultural and Ecological Warfare

- **Don't get mad get even – revenge is a dish best eaten cold.**
- **Already have many inadvertent cases to show this threat is real.**
- **If state-driven or well-organized attack, can be highly sophisticated, long-delayed, very hard to detect, and very hard to attribute.**
- **Advances in bioattack and biodefense technology are just as important here.**
 - **Syndromic surveillance and improved detection?**
 - **Response technology?**

CYBERWARFARE VS. CYBERTERRORSM

Asymmetric Warfare: What Does Cyberwar Really Mean?

- **We need a clear picture of current and projected cyberwar options for attackers.**
 - **Effective defense and response requires a full-scale net technical assessment of what attackers can really do, key vulnerabilities, and requirements for defense and response.**
 - **Exercising responses to assumptions about such attacks is not analysis or adequate planning**
- **Cyberwar can occur at a number of levels and in conjunction with other means of attack.**
 - **A covert cyberwar may be possible where the attacker cannot be identified quickly or at all.**
 - **Larger-scale cyberwar may involve clearly identifiable attackers.**
 - **Given the low cost of cyberwar, is a missile or CBRN attack without cyberwar credible?**

Asymmetric Warfare and Attacks on CIP/Information Systems

- **Cyberwar is *not* cybercrime or cyberterrorism**
- **Refocus on critical threats, leave normal defense to private sector, state/local, and federal agencies.**
- **Identify true critical risks. Look at cases where basic reductions in technological vulnerability may be the only solution**
- **Examine the full range of legal changes necessary for effective defense, including the “laws of war.”**
- **Conduct a Zero-based reexamination retaliatory and offensive options.**
- **Force the creation of a common future year program with honest deployment and life-cycle costs.**
- **Examine the real-world limits of intelligence, warning, and defense.**
- **Require Net Technical Assessment and realistic evaluation of cost to defeat proposed programs and solutions as part of this zero-based options.**
- **Conduct a “zero-based” review of legislation to clearly define how intelligence and law enforcement can be made more effective, and the trade-offs involved.**
- **Evolve the right solution to real problems.**

Asymmetric Warfare and CIP/Information Systems: Is There an Offensive Option?

- **“Technology 101” at the defender level says you really cannot identify the attacker and respond:**
 - **Can a 21st Century approach change this?**
 - **If so, in time to actually defend or in time to retaliate?**
- **What is the difference between “cyberattack” and “cyberwar”? When does the level of attack become wide or critical enough to merit decisive federal action?**
 - **Is some form of national cyberwarning possible? Can you characterize attacks well enough to know the difference? Is some form of cyber damage assessment in near real-time possible? Can you build a warning system and net into critical national networks?**

CIP/Information Systems: the Need for Degenerative, Non-Vulnerable, and Replaceable Systems

- **There is far too much emphasis on trying to shield entry to highly distributed fragile or vulnerable systems.**
- **The only workable solution at many levels may be to avoid over-dependence on systems that cannot function in a degenerative form, are not sealed off, and do not have some workable human alternative.**
- **Alternatively systems must be designed to survive prolonged crashes, and be reconstitutable.**
- **Current diagnostics overemphasize guarding the portal, rather than measuring broad systematic attack patterns. Integrated and systems-wide warning and diagnostics are needed.**

IMPLICATIONS FOR MANAGING DEFENSE

Asymmetric Warfare: Timelines and Responsibility

- **Must have strong DoD Element: Offensive and theater focus equally important, foreign intelligence critical**
- **Need effective 5 and 10 year programs based on realistic threats, not short-term half-measures in response to artificial crises.**
- **Some kind of central planning and programming is critical, but the issue is not strategy, masterminding today's defense/response, or allocating one rear of budget funds. Must develop and manage a coherent program in detail.**
- **Who and where the Czar is, is important. What the Czar does is far more important.**
- **Must be central managers for intelligence, defense, and *response with individual programming and review authority and adequate resources*. Putting some one in charge at the top is of limited practical value unless this is done.**
- **Need to understand that no affordable system is likely to be capable of dealing with worst cases, and no one will pay for worst cases until the threat is far more tangible.**
- **Congressional review cannot be improved until the Executive Branch presents a program worth reviewing.**

ⁱ See USACHPPM, The Medical NBC Battlebook, USACHPPM Technical Guide 244, Section 2, Field Manual (FM) 1.1-31-2, FM 3-7, and FM-8-10-7.

ⁱⁱ USACHPPM, The Medical NBC Battlebook, USACHPPM Technical Guide 244, p. 2-6.

ⁱⁱⁱ USACHPPM, The Medical NBC Battlebook, USACHPPM Technical Guide 244, pp. 2-6 to 2-23, and 2-28 to 2-29, FM 8-9, Table 6-II, and FM 8-10-7, Table 4-2.

^{iv} USACHPPM, The Medical NBC Battlebook, USACHPPM Technical Guide 244, pp. 2-5 to 2-23.

^v USACHPPM, The Medical NBC Battlebook, USACHPPM Technical Guide 244, p. 2-15.

^{vi} See AFRRI, AmedP-6©, and USACHPPM, The Medical NBC Battlebook, USACHPPM Technical Guide 244, pp. 2-15

^{vii} These issues are poorly dealt with in most weapons effect manuals, but are discussed in summary form in Office of Technology Assessment, "The Effects of Nuclear War," Washington, US Congress, OTA-NS-89, May 1979.

^{viii} USACHPPM, The Medical NBC Battlebook, USACHPPM Technical Guide 244, p. 3-16 to 3-17; Joint Publication 3-11 (Draft), FM-8-9, FM 8-10-7, AMEED Center and School's, Effects of Nuclear Weapons and Directed Energy on Military Operations, and DoD 5100.52-M Nuclear Accident Response Procedures Manual – NARP.

^{ix} See AMEED Center and School, Effects of Nuclear Weapons and Directed Energy on Military Operations, (especially p. 1-34) and USACHPPM, The Medical NBC Battlebook, USACHPPM Technical Guide 244, pp. 3-15 to 3-16.