Countering Traumatic Attacks*

RICHARD DANZIG

For millennia, offensive warfare has aimed to destroy, degrade, or capture an opponents' troops weapons, property, and territory. Since the invention of gunpowder in the mid-14th century, the main means of doing this has been by explosive weaponry: bullets, bombs, mines, and missiles. Another risk to American security over the next decades is that both this aim and these means may change. The aim will not be to destroy American military power (that's too difficult), but rather to sap the will to use it. The means will be nonexplosive warfare, conducted with NEW weapons. The manifestation of these changes will be "traumatic attacks."

How do NEW weapons differ from their predecessors? What special aims of traumatic attacks are amplified when these weapons are used? What kinds of investments would diminish risks from these weapons and these types of attacks? This chapter describes three broad changes, going well beyond our traditional reliance on deterrence, that are likely to be necessary if we are to maintain our security in the 21st century.

In the late 20th century, traumatic attacks have predominantly employed explosive munitions placed in or near buses, cars, airplanes, and buildings. Accordingly, we now focus on explosives when we attempt to protect the security of airports, military bases, government buildings, and other key facilities and means of transport at home and abroad. At the same time, we are making well-warranted efforts to reduce and control the world stockpile of nuclear weapons.

The dangers of the future, against which we are underprotected, arise from NEW weapons, predominantly biological and information warfare, secondarily from chemical or radioactive materials. Attacks of this kind are less familiar but have grave potential for causing mass disruption, panic, and (in the case of biological weaponry) deaths that could be counted in the hundreds of thousands.

An understanding of the most novel activities, biological and information warfare, will illuminate the character of these weapons.[1] Biological attack is the dissemination of bacteria, viruses, or toxins to cause debilitating or fatal illness through breathing, drinking, or absorption. Weapons of this kind are extraordinarily potent. It has been calculated that a millionth of a gram of anthrax will first sicken and then, within a week, kill anyone who inhales it; taking account of dissipation and delivery over a metropolitan area, a kilogram has the potential to kill a million people.[2] If an infectious agent like plague or smallpox is used, a chain reaction can be induced, and the effects of an incident may be unbounded. Beyond its ability to kill, a biological attack can be highly distruptive. Sickness induces panic and psychosomatic effects. Large numbers of

This article was originally published as part of *The Big Three: Our Greatest Security Risks and How to Address Them* (Washington, D.C.: National Defense University, 1999), pp.37-49.

people in panic, flight, and illness can quickly overwhelm our regular systems of care, transportation, and communication.

It is striking how analogous information attacks are to their biological counterparts. We even use similar terminology when we describe a computer "virus." A single computer virus, like its biological equivalent, can have widespread and proliferating effects. Whether embedded in software in advance or disseminated near the time of use, a computer virus can destroy or distort data in the information and communication systems upon which military and civilian life depends. The gravity of the Year 2000 problem--a "natural occurrence" that corresponds to information attack, as natural outbreaks of disease do to biological warfare-- highlights our dependence upon, and yet the vulnerability of, information and communication systems.

Biological and information attacks share more than a dozen characteristics that can make future security problems very different from today's. These attacks will not depend on, or be defeated by, mass, either of armies or of physical barricades. They do not require large, visible methods of production. Potent biological weapons can be made in a room and held in a vat. The forces of cyberspace can be marshaled on a desk and stored on a disk. The skills and assets required to wage this kind of war are very like those associated with legitimate civilian activities in the pharmaceutical and computer industries and are rather readily and inexpensively obtained. Once prepared, these weapons will not require missiles, shells, or other very visible, technically demanding, or expensive methods of delivery.

A single computer can launch an information attack. An ordinary crop sprayer can generate a fatal anthrax cloud over 80 miles long. A single leased airplane dispersing a biological agent can kill more people than died in any month of World War II. The effects of these attacks can occur for substantial periods after delivery, and consequences must be measured by the uncertainty, panic and physical effects they will cause.

Distinguishing among crime, terrorism, natural occurrences, and war become difficult when NEW weapons are used. Because large financial resources, massing power, and delivery systems are not required, it is not necessary to be a major nation to be able to conduct this type of warfare. Though subject to use by a major competitor, second- or third-tier states, subnational groups, or even individuals may present threats from biological and information warfare. A large industrial base is not required to develop or deploy NEW weapons, because they are postindustrial weapons; in the postindustrial era, the power to wage war is no longer monopolized by nation-states.

Furthermore, the characteristics of low visibility, delay, and natural occurrence can be exploited to leave uncertainty as to whether a military attack occurred and, if it did, who conducted it. This makes retaliation difficult. Because deterrence depends on a credible ability and will to retaliate, deterrence will not be as effective in suppressing traumatic attacks as it is in discouraging other forms of warfare.

These are fast-growing technologies. While explosive weapons and their delivery systems take decades to evolve and produce, NEW weapons multiply in variety and potency with a speed that characterizes the biotechnology and software industries from which they stem. Defenses typically cannot keep pace with offenses that are so easily varied and proliferated.

Taken together, more than a dozen attributes differentiate these weapons. They cannot be countered by the usual methods. Worse still, we are handicapped in recognizing changes needed to counter these weapons. The military establishment is not attuned to these issues. The familiar weapons are explosive weapons. The familiar battles are the clash of armies, navies and air forces. Familiar battlefields are the places where militaries grapple with their opposite numbers. The traditional business of warfare is explosive weaponry, not disease (the province of doctors) or information (a support function). Further, we do not have well-developed offensive programs that might inform and stimulate our defensive efforts. Since 1969, we have refrained from any offensive program involving biological weapons. The decision to refrain from an offensive program, though appropriate, is like the amputation of an arm; the military is struggling to grasp a load with one hand when it is used to using two. The offensive possibilities of information warfare are more readily understood, but, in part because of our own vulnerabilities, we are inhibited about practicing and openly debating the offensive aspects of information "traumatic attack."Consequently, in this area also, our ability to grasp the risk (and to counter it) is weak.

For their part, civilian authorities are not used to looking upon their domains as battlefields. The FBI is concerned with developing criminal cases; the Center for Disease Control, the Public Health Service, and local power companies are focused on natural events, not defense against attacks. Our military and civilian agencies are not commonly or easily coordinated. We are, in short, ill positioned for coping with NEW weapons and most especially so if these weapons are used in "traumatic attacks" against our civilian populations.

NEW weapons can be employed in traditional military settings or to undermine reinforcement and to mass in preparation for conventional warfare. But both biological and information warfare is more potent in less conventional circumstances: it can be used to gain bargaining leverage by threatening civilian populations and to induce a distracting and dispiriting panic in those populations. However vulnerable troops and military information systems may be, civilians are vastly more so. While military forces enjoy a modicum of protective clothing, encrypted systems, and other barriers to biological and information attack, civilian populations are highly vulnerable. Troops are trained and disciplined for combat; civilians, especially American civilians, are not prepared.

Warfare aimed at civilian populations would not be assessed by body counts or territory occupied, but by how the minds of the American public and that of allied populations were affected. Alvin and Heidi Toffler have pointed out that ways of making war reflect ways of making wealth.[3] In an agricultural age, battles were fought with agricultural instruments (such as horses and swords), the unit of value was land, and victory was achieved by occupation of territory. Industrial-era wars are fought with the products of industry (for example, engines and explosives), and victory is achieved by destruction. In the information age, information and telecommunications are likely to be principal weapons, and molding perceptions may constitute victory.[4]

We have not yet reached the point where perceptions can be molded without events. Traumatic attacks are the thin end of the wedge by which public opinion can be leveraged, the hook on which perceptions can be hung. The hallmark of these attacks is that they are valued not for their physical effects but for their psychological consequences. It was not the occupation of territory or the disablement of the American military machine that determined the value of the Tet Offensive in Viet Nam, the bunker bomb in Lebanon in 1983, or the massacre of soldiers before CNN cameras in Somalia in 1994. Of course, traumas can have the opposite effect and instead multiply national determination; the Alamo, the Maine, and Pearl Harbor became rallying cries precisely because of the injury they inflicted. But these were not designed to be traumatic attacks. In retrospect, we can see that the attackers did not understand the psychological consequences of achieving their material goals. These experiences warn the designers of traumatic attacks that they are working with a most potent power that may backfire or get out of control in unexpected ways. The handling of the consequences of events may be more important than controlling the events themselves.

A first and right instinct is to protect ourselves against the NEW weapons. Though we cannot be totally successful in these efforts, we can do a great deal. To defend against biological attack, we can secure large benefits from rapid development and deployment of detector technology; investment in antibiotic and vaccine research; stockpiling of medicines and vaccines; inoculation; refinement and acquisition of simple form-fitted masks to prevent infection by inhalation; improved intelligence, enhanced training; and development of doctrine about how to preempt and, when necessary, respond to a biological attack.

Our defense against information warfare similarly demands more innovative preparation. Our aim should be to prevent intrusions and alterations of data that can misdirect missiles, airplanes, ships, and spare parts and distort financial, utility, telecommunication, and other systems upon which we depend. A deeper perception of these vulnerabilities should lead to greater investments in intelligence and in research and product development for computer and communications security. We should reflect the state of our defenses against these vulnerabilities in our readiness systems, include it in the training of officers, and exercise information protection along with our other defensive skills.

Our efforts to defend against traumatic attacks, however, demand more than the application of these traditional approaches to the new areas of biological and information warfare. Above all, they demand challenging shifts in our conceptual framework. In addition to defense, we need to tailor strategies of dissuasion, deterrence, disruption, and consequence management to the challenges of NEW weapons.

To reduce the risk of a military competition, a theory of dissuasion needs to take its place alongside theories of deterrence. Dissuasion seeks to avert the development of a major military competitor; deterrence seeks to limit the actions of an established competitor. NEW should emphasize the benefits of pursuing dissuasive strategies even with nations that are not likely to be major competitors. Because NEW weapons can be used or proliferated by second- and third-tier states-even, for example, by a poverty-stricken Korea or an isolated Iran-there is a security reason for trying to tie these states into the community of nations. To counter weapons of mass disruption, it is desirable to bring countries that may be opposed to us to a point where they have a stake in maintaining the world system and thus in avoiding disruption.

Working from a position of military and economic superiority, we can afford, and in our own interests should pursue, openhanded, cooperative strategies that avoid creating pariah states. We are given a further opportunity to do this with NEW weapons. We can, and should, forge a world consensus that emphasizes the moral unacceptability, and therefore the cost in public opinion, from using weapons of this kind. Moral opprobrium is hardly a reliable barrier, but it has dissuasive power, particularly when it must be considered by terrorist groups seeking to establish the legitimacy of their cause.

Where dissuasive strategies do not succeed, we will, and should, rely on deterrent policies. However, strategies of deterrence must be extended and reworked to take account of the likelihood that terrorist groups and individuals are among potential users of NEW weapons. Deterring those actors (and their acquisition of NEW weaponry) is different from deterring state actors. We need to understand the psychology and structure of nonstate groups and recognize that old techniques (threats of nuclear retaliation, for example) typically will not work against them.

When confronting terrorist groups (and some resolute second and third-tier states), disruption may be a more important strategy than deterrence. While deterrence threatens reaction, disruption is proactive: it intrudes upon would-be attackers, with preemptive strikes, inspections, arrests, or such pressure of detection and restriction on freedom of movement as to thwart intended strikes. Our society is uncomfortable with disruption: it threatens civil liberties, risks alienating public opinion (or creating martyrs) through heavy handedness, provides little assurance of success, and commits us to innumerable small battles without the likelihood of eradicating threats. It is, however, an essential tool against terrorism. We need to develop strategies of disruption that are closely controlled by civil authorities, narrowly targeted to thwart traumatic attacks by the least drastic means, and compliant with our own and international laws.

Beyond this, a fourth approach is needed to complement deterrence, dissuasion, and disruption--"consequence management." This approach would develop procedures and resources to limit the effects of attacks. Consequence management is required because our reliance on information systems will, over the next decades, persistently outrun our abilities to protect these systems completely. Similarly, biological, chemical, or explosive attacks will be so easily mounted, against targets so numerous and so exposed that society cannot be insulated completely against this trauma. Defense, dissuasion, deterrence, and disruption are worth substantial investment, but our working hypothesis ought to be that, despite our best efforts, successful traumatic attacks will occur.

Accordingly, we should invest in managing the consequences of attack so as to reduce the resulting trauma. By this means we will also diminish the incentive for opponents to utilize this form of attack. In the information context, this requires designing systems that are redundant and compartmentalized so that, when successfully attacked, failure is 'graceful' rather than catastrophic. It involves the design of data systems that are camouflaged to confuse intruders, tagged and encoded to detect manipulation, and encrypted to minimize the benefits of intrusion.

In biological defense, consequence management requires investments in our public health systems. We need standby medical capabilities so that attacks can be promptly recognized and therapeutic regimes initiated before symptoms become pernicious. In both information and biological defense, consequence management must include the creation of public and military information systems to diminish panic and confusion.

Such an approach to consequence management must also carry with it a rethinking of the anachronistic distinctions between "here and abroad" and between military and civilians. Traumatic attacks that threaten our national security may be aimed at our troops and allies abroad, but they are as likely to be aimed at people and activities based in the United States. Certainly, cyberspace has no geography, and anyone who doubts that biological agents can easily be imported into the United States need look no further than the flow of drugs into this country. Once imported (or obtained), biological agents are easily disseminated by use of readily available crop sprayers and other such devices. Boundary defense cannot be relied upon to defend against cyber invasion or biological agents.

Investments in protecting civilians against these untraditional threats have a rationale and benefit not present when considering civilian protection against conventional weapons. Illness occurs naturally, and information security is challenged every day in our economy; therefore dollars used to protect us in these arenas yield everyday rewards. "Civil defense" expenditures may be questioned, but by contrast, "public health" investments (for example, in the Centers for Disease Control and the Public Health Service) and information security investments are well warranted for coping with natural as well as military contingencies.

When dealing with NEW weapons, a line of separation cannot be drawn between military and civilian systems. Our ability to project military power depends, both here and abroad, on civilian utility, transport, telecommunications, and finance systems, which in turn depend on properly functioning civilian information systems and civilian employees. All can be undermined or overwhelmed by driving massive numbers of civilian populations away from or toward centers of activity. It is not likely that our response to a biological threat against Denver would, or should, be limited to the Denver Police Department, or even the FBI and Federal Emergency Management Agency. Nor could we ignore such threats against civilians in host nations that receive and sustain our forces when they are deployed abroad.

Sustaining our military power requires dealing with the consequences of traumatic attack. To do this we will have to focus on NEW weapons, in addition to explosive weapons; on terrorist groups and individuals, as well as major powers; on consequence management, as well as on defense, dissuasion, deterrence, and disruption; on civilians and civilian systems, not just military personnel and operations; and on our vulnerabilities at home as well as abroad.

Notes

1. Biological weapons are novel but not unprecedented. In the Middle Ages, bodies were catapulted over the walls of castles under siege in order to spread plague; in America's French and Indian wars, Indians were given blankets infected with smallpox; in our Civil War, Sherman's march to the sea was impeded by poisoned wells; and in World War II, Japanese Unit 731 experimented with biological weapons that killed as many as a thousand Chinese civilians.

This subject is, for expository purposes, given limited space. Other types of NEW weapons should not be overlooked. Chemical weapons, the most pervasive and familiar, are somewhat more confined in their likely effects. They are also relatively easy to focus and control. Accordingly, they may be the most likely to be used. Radioactive weapons (though not necessarily explosive) lie at hand wherever there are large nuclear programs, whether developed for peaceful or military purposes. In Russia, perhaps the greatest source of risk in this regard, there are estimated to be some 2.5 million pounds of enriched uranium and plutonium. More than half of that is embedded in some 24,000 nuclear weapons, and 12,000 in storage. The balance of this weapons-grade material is in more than 50 military and civilian research institutes. With so little state power and economic well being in Russia, there are high risks that this radioactive material will be bought or stolen and used for traumatic attack.

2. The appropriate absence of an offensive program and limited test information and experience make these estimates subject to debate.
3. *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown and Company, 1993)
4. Warfare of this kind is certainly not unprecendented. The allied strategic bombing of Germany and our use of atomic bombs against Japan were aimed, at least in part, at demoralizing our opponents.

*This article or chapter may be found in Max G. Manwaring (ed.), *Deterrence in the 21st Century*, London: Frank Cass, 2000, pp. 98-105.

OSS '03 PROCEEDINGS "BEYOND OSINT: Creating the Global Multi-Cultural Intelligence Web" - Link Page

Previous	OSS '03 David Boren, Foreword, The Search for Security: A U.S. Grand Strategy for the 21st Century,
Next	OSS '03 Michael Andregg The State of the Academic Tribe in 2003 (Text),

Return to Electronic Index Page