

**Terror in the Suites**  
**Narratives of Fear and the Political Economy of Danger**

Ronnie D. Lipschutz  
Associate Professor of Politics  
260 Stevenson College  
University of California, Santa Cruz  
Santa Cruz, CA 95064  
Phone: 831-459-3275/Fax: 831-459-3334  
e-mail: [rlipsch@cats.ucsc.edu](mailto:rlipsch@cats.ucsc.edu)

**Abstract**

In this paper, I propose that we are increasingly subject to a "political economy of danger." In using this term, I do not mean to suggest that terrorists, whether foreign or domestic, have somehow gained power over our lives and destinies; rather, I mean to suggest that the fear of things unknown, unseen and unexpected has come during the 1990s to play a central role in the politics and economy of the United States. Indeed, the political economy of danger plays a dual role in the life of our society. On the one hand, it is critical to the production and reproduction functions of those arms and agencies of government and society concerned with security and corrections, both domestic and foreign. On the other hand, in a society made increasingly unruly by marketization and social change, a political economy of danger provides a mode of social control and a rationale for the surveillance necessary to maintain discipline, based on what is known and what is not; what is knowable and what cannot be known. It derives directly from the media's search for market share and the ease of extrapolation from events that have taken place to those that are, as yet, only imagined. Things are reported; much is unknown; speculation is rife; conclusions are drawn. Often, these conclusions are wrong, but that does not matter. It is the initial impression that counts, not the causality; it is the flash and bang that draws attention, not the detailed minutiae that follow from the long, drawn-out investigation. And it does not take much to create the impression that one event is representative of a category that is bound to happen much more frequently, even if that event is a singular one with no resemblance to the others of which it is said to be an avatar.

**Terror in the Suites**  
**Narratives of Fear and the Political Economy of Danger<sup>1</sup>**

Ronnie D. Lipschutz

*“Evil has been with us since the first man was born, and there are many, many evil people out there that don’t use the telephone, that don’t talk to reporters, that don’t broadcast their intentions, and it is absolutely essential that we have the capability to prevent, for instance, another World Trade bombing, only this time with a nuclear bomb, a destruction of the Federal Reserve by an attacker going against their computers, the release of a biological weapon in Los Angeles. These are things that originate overseas, and if we don’t have spies, then we are vulnerable to catastrophic failure, catastrophic attack”<sup>2</sup>*

Robert Steele, CIA Officer, 1979-80(??)

**STORIES TORN FROM THE HEADLINES...**

On July 17, 1996, TWA 800 took off from John F. Kennedy airport in New York, bound for Paris. A few minutes into the flight, the Boeing 747 was ripped in two by an enormous explosion amid-ships. The front part of the plane plunged into the ocean below; the rear section continued to fly for a few more minutes before it, too, fell into the waters off of Long Island. Two hundred and thirty people died. Almost immediately, the government and media blamed the disaster on a terrorist bomb, probably of Middle Eastern provenance; this was soon countered on the Internet by conspiracy theorists who blamed the U.S. Navy for shooting the plane down (something that had once happened in the Persian Gulf). Two years of intensive examination of the plane's remains, however, failed to provide evidence of a bomb or missile, and investigators concluded that an electrical spark in the almost empty center fuel tank had ignited fuel vapors and set off the explosion. Despite indications that no humans were involved, the event nonetheless was offered as an example of the vulnerability of contemporary air travel to terrorist attacks. One result--which did not change as a result of the investigation--was a program implemented by the Clinton Administration that would

create a special computer tracking system to flag, or ‘profile,’ passengers and identify those with suspicious travel patterns or criminal histories.... The names addresses, telephone numbers, travel histories and billing records of passengers would be run through a giant database that might lead to a search of the luggage of those deemed suspicious.<sup>3</sup>

\* \* \*

According to a 1993 OTA study cited by Richard Betts in a recent article in Foreign Affairs, "a

single airplane delivering 100 kilograms of anthrax spores...by aerosol on a clear, calm night over the Washington, DC, area could kill between one million and three million people." There is, he and other claim, a good chance that such an attack will take place sooner or later, and the American public remains largely unaware of this threat and sleeps soundly when it should not. Evidence in support of Betts' warnings was not long in coming, it would seem. On February 19, 1998, two men were arrested in Las Vegas for alleged possession of anthrax. According to an FBI informant, one of the two had bragged that he had enough of the virus to "wipe out the city," although it was not immediately clear whether the confiscated material was, indeed, viral. A mild panic ensued because, as the Las Vegas Sun put it, "The...arrests came as the country prepares for possible military action against Iraq's Saddam Hussein, who is suspected of manufacturing biological weapons such as anthrax." The Sun failed, however, to explain how the two were connected. Subsequent examination of the substance revealed it to be not the bug itself, but a greatly-weakened version used as a vaccine against anthrax in animals. Even so, the incident became one more data point for those who argue that Americans must take defensive precautions because it is "only a matter of time" before terrorists attack an American city with biological weapons. During December 1998 and January 1999, there were more than a dozen warnings of anthrax attacks in the Los Angeles area; all were hoaxes.

\* \* \*

On March 11, 1998, Dr. Brian G. Marsden, an astronomer at the Smithsonian Astrophysical Observatory in Cambridge, Massachusetts, issued a report warning about an asteroid that might come perilously close to Earth in 2028, perhaps passing within the moon's orbit, possibly even striking the planet. For the next day or so, extensive discussions were to be found in the media and on the Internet, with warnings that, as went the dinosaurs 65 million years ago, so could we. Advocates of developing a defense against such interplanetary objects--many of whom were also supporters of the Strategic Defense Initiative (the advocates, not the asteroids)--warned that, without adequate space-based preparation against such extra-terrestrial threats—and given that we are very close to the 65 million-odd years between major strikes--our number will eventually be up. Subsequent examination of Marsden's calculations by other astronomers and astrophysicists suggested that he was in error and that said asteroid would miss the Earth by quite a few million miles. Nevertheless, NBC rebroadcast its TV movie about asteroids hitting the Earth, and during the summer 1998 movie season, two commercial films on "E.L.E.s" (extinction level events) were released to an eager public.<sup>4</sup>

\* \* \*

These days, there is no shortage of such stories. They are based on "real events," torn from lurid headlines (*How Japan Germ Terror Alerted World*<sup>5</sup>) over media reports on threats posed by a dangerous world. Yet such stories are as much about myth, trope and narrative as they are about "news" and "reality." To be sure, they involve living people, material objects and real events; they posit mortal risks to part or all of the body politic; they trigger major responses or debates about security, protection and prevention; they are, nonetheless, what I call narratives of fear, stories of danger. We, The Living, have escaped--so far. The next time--perhaps even tomorrow--we will not: then, the bomb will be real, the virus will kill, the comet will hit (*News at 11!*). Because such incidents are sure to happen, we are told by the authorities (and authors of these stories), we must be prepared and ready. Lacking readiness is to court misfortune,

instability, danger, death: “catastrophic failure, catastrophic attack,” as ex-CIA officer Steele would have it. Having produced both fear *and* prudence in the listening audience, those same author(itie)s assure us of protection—if, of course, they are provided with appropriate resources—thereby guaranteeing the public a peaceful sleep. (In any event, would such protection even be offered were the dangers not real and imminent? Anyway, it’s cheap insurance for both mind and body.)

The threats, risks and hazards reported in such stories are neither wholly implausible nor without potential danger; certainly, similar incidents have *already* happened. After all, the dinosaurs died after a comet hit the earth 65 million years ago. Pan Am flight 103 fell from the sky over Lockerbie, Scotland ten years ago when a booby-trapped tape recorder blew up in the baggage compartment. Commuters in the Tokyo subway died from exposure to sarin nerve gas four years ago when it was released by the Japanese sect Aum Shinrikyo. It is said that the World Trade Center came perilously close to being toppled five years ago when a van exploded in one of its parking garages. But such episodes are manifestly uncommon and, excepting comets and asteroids the “size of Texas,” they are rather selective and limited in their impacts. Indeed, the risks of dying by a terrorist’s hand or bomb are extremely small (less than dying from an accident in one’s home). So why such great concern today, in the waning days of the 20th century? And why such a willingness to accept at face value the stories told about these dangers, especially in the face of more manifestly unhealthy risks that are much more common, predictable and controllable?

In this article, I consider such questions. I do this through an examination of the way in which truths and narratives of fear are *produced*, and of the political economy of danger that results. The threats might be out there, or they might not, but I do not mean to assess their veracity here, in any case. Rather, I take to heart David Campbell's admonition that "Danger is not an objective condition. It is not a thing which exists independently of those to whom it may become a threat."<sup>6</sup> My interest here is not the carnage and political upheavals that could, according to those who claim to know, result from an anthrax release in, say, Los Angeles. Instead, I am concerned with *how* such fears seep into the consciousness of the body politic and generate self-perpetuating systems of ideological and material production and reproduction. Keeping Campbell's warning in mind, I argue in this paper that the proliferation of new threats and dangers during the 1990s is not the result of their sudden, or even gradual, appearance on the world political scene. Instead, I propose that the production of these particular truths and the narratives of fear and political economy of danger that follow are attributable to a "world turned upside down" by globalization and the social uncertainty it has generated (a phenomenon that is not a new one, not even for the passing century). Moreover, these truths are generated through practices and settings similar to those described by Bruno Latour and his associates in their studies of “science in action.”<sup>7</sup>

I begin with a general discussion of security threats and then focus on recent discussions of two specific categories: "cyberwar" and biological terrorism. I also ask: "What do we know? What is the *empirical* basis for the claims made that these are imminent dangers?" While I have no way of evaluating the substance of the truth claims that are made about these threats, it is not clear that the empirical data used to validate them are significant, as opposed to signifying. In the second part of the paper, I examine more closely the mechanisms through which narratives of fear are produced, again through the two examples of cyberwar and biological terrorism. The third part of the paper addresses the material basis of the truth production system, centered in

what I call the "political economy of danger." Finally, in the last part of the paper, I ask whether the "State of Terror," as Annamarie Oliverio has so nicely put it,<sup>8</sup> is an inevitable part of our lives and one with which we are destined to live or whether it is possible to explain the "terror in the suites" in more prosaic and, therefore, less inevitable terms.

## THE PRODUCTION OF TRUTHS AND NARRATIVES OF FEAR

November 1999 marks the tenth anniversary of the "end" of the Cold War, yet a sense of apprehension and insecurity is abroad in the land: there is no Enemy. Although NATO's air campaign over Yugoslavia, and various reports telling of Chinese nuclear espionage suggest that new Enemies might be a-building, for lack of a coherent, consensual "threat," the basic premises of U.S. national security policy continue to be uncertain and ill-defined.<sup>9</sup> No agreement on the nature or source of present or future threats has developed<sup>10</sup>; no comprehensive strategy akin to containment has emerged<sup>11</sup>; no clear-cut policies regarding force structures and deployments have been formulated.<sup>12</sup> Instead, there is an on-going search for problems of sweeping scope that might provide strategic coherence and force discipline on an apparently unruly polity and evidently disorderly world, complemented by a seemingly-endless debate about how to meet the panoply of new threats that have been discovered.

Among the dangers said to be facing the United States are the following: economic competition from former clients, both countries and corporations<sup>13</sup>; regionally-threatening rogue states and globally-threatening "civilizations" bent on upsetting the international order<sup>14</sup>; shadowy possessors of nuclear-tipped missiles targeted on U.S. allies, troops and cities<sup>15</sup>; religious zealots and terrorists of mostly foreign origin bent on seeking revenge for all sorts of slights and abuses<sup>16</sup>; illicit, youth-destroying drugs shipped and marketed by cartels and transnational criminal networks that literally control entire countries<sup>17</sup>; computer hackers in the employ of hostile governments and sub-national entities bent on cyberwar and cyberterror (see below); illegal immigrants stealing both natural and fiscal resources while engaged in undermining national culture; environmental catastrophes<sup>18</sup>; exploding cities<sup>19</sup>; encroaching plagues<sup>20</sup>; corrupting influences<sup>21</sup>; even, as noted above, Earth-bashing comets and asteroids.<sup>22</sup> Some analysts refuse to be so specific, arguing instead that the enemy is instability, uncertainty and disorder;<sup>23</sup> others warn that the world is a dangerous place full of "wolves in the woods"<sup>24</sup>; a not-insignificant number even argue that the real threats arise from enemies "within," bent on cultural corruption, sexual perversions, bad government, and Marxist tendencies.<sup>25</sup>

Expansion of the national security agenda to encompass a broad range of issues and problems is hardly a new practice; many can remember the 1950s and 1960s, when education, health, civil rights and highways were brought under the national security blanket, ostensibly as part of the conflict with Global Communism but also as *sub rosa* form of military Keynesianism. The contemporary search for threats differs, however, from the hysteria surrounding Sputnik, Race Relations and the New Math. This one has a rather different and more frantic quality about it, as though even those seeking to unmask imminent dangers lack the conviction that they are "real," the way the nuclear threat was deemed to be "real." Alternatively, perhaps it is that the search for the Great Threat--the "Great Whatsit," as Mike Hammer's girlfriend Velda puts it in the 1955 film *Kiss Me Deadly*--is a proxy for some other social lacuna or anxiety.

Nevertheless, uncertainty, however great it might be, demands a response it would seem. A failure to be prepared for any and all contingencies carries with it the risk of another "Pearl

Harbor," or worse (as we shall see). But the contradiction is clear: Full security demands a high degree of certainty, one that is virtually impossible to achieve, while there is much uncertainty in the ideologies by which we chart our lives and in the ways we live them. Risks can never be fully domesticated. Moreover, as risk analysts often point out--and Reagan-era military expenditures suggested--attempts to achieve zero risk and full security are a sure path to bankruptcy. Fifty years ago, George Kennan cautioned that, in a world of limited resources and (apparently) unlimited threats, we would be tempted to prepare for every contingency, no matter how remote. It would be better, he argued, to match threats to resources.<sup>26</sup> If, at a minimum, we are to hew to his advice, we should at least understand what we think constitutes a threat, and why it does (if it does).

The description of a world of threats leads, however, to a second question: How do we decide what constitutes a threat worthy of national attention and expenditure? Certainly, in today's world, there is no shortage of banal and widespread threats to health, welfare and infrastructure, or sources of abuse, injury and death. Poverty, polluted air and water, toxic waste, cigarettes, automobiles, small arms, large arms, teens, neighborhood violence, spousal abuse, backhoes cutting major telephone cables, fallen branches downing critical power lines, line workers blacking out cities (electro-terrorism or just "human error?") and selling bomb-making materials (chemo-terrorism or just the "entrepreneurial spirit?"), malfunctioning satellites--the list seems endless. Some of these dangers are random and unpredictable, but many are amenable to treatment and could be addressed, saving tens or even hundreds of thousands of lives per year,<sup>27</sup> more than have ever been lost to terrorism, to pick one much-feared national security threat.

Instead, it is the narratives of fear emanating from *authorized* sources that have attracted the growing attention and resources of the state and associated institutions.<sup>28</sup> Why? Several possibilities suggest themselves. Perhaps the threats about which we are warned *are* "real" and could become material and manifest at any moment. But as I suggested above, our everyday lives are full of manifest risks and the consequences of ignoring them. Even though there are public campaigns against smoking, handguns, drinking and driving, and a myriad of others, none has quite the same cachet as the threat from the unknown and unpredictable.

Perhaps, life has become so safe, yet technologies so complex that, as Ulrich Beck argues in *The Risk Society*,<sup>29</sup> people are increasingly sensitive to ever-diminishing risks that seem to pose ever-larger and catastrophic consequences. They are especially sensitive to those over which they exercise no control.<sup>30</sup> Yet, while there is a myriad of social movements organized in opposition to such problems as nuclear power, genetically-engineered vegetables, and urban toxics, no corresponding groundswell is evident where biological terrorism, cyberwar, global crime or other such phenomena are concerned.

Possibly the problem has to do with our responses to notions of *threat* and *security*, both national and individual. According to people in the know, the most-feared scenarios of catastrophe could, were they to occur, undermine national cohesion and legitimacy and cause widespread panic, death and destruction; they are to be greatly-feared.<sup>31</sup> In the past, widespread fear was addressed by "domesticating" national security threats, and getting people used to living with them. The 40-year nuclear standoff between the two superpowers, carrying with it the potential for mass annihilation, was certainly fearful. Nevertheless, when *that* fear was given voice by a skeptical public in the campaigns against nuclear testing and weapons, it was pooh-poohed by strategists and policymakers.<sup>32</sup> Today, the new threats are propounded and

magnified, in many instances by the very same people who domesticated the nuclear threat, with the express purpose of terrifying the public and eliciting political demands for action.

Perhaps the proliferation of security threats has ontological roots, constituting not so much an attempt to *protect* society from harm as to *discipline* in the face of a "new world disorder" that has begun to destabilize social hierarchies. Perhaps the disappearance of a singular enemy deemed responsible for all the world's evil and danger has left an insecurity vacuum of sorts. Perhaps this void must be filled in order to restabilize authority and relegitimate discipline.<sup>33</sup> There is something to this last explanation, but it gives too much to ideology and not enough to material factors.

This suggests that the process whereby contemporary national security policy is being made is not so simple as discovering and specifying "threats" but also involves their creation (and marketing?) out of what I have elsewhere call "imagined futures."<sup>34</sup> Indeed, the epistemological and practical difficulties that have arisen in "redefining security"<sup>35</sup> suggest that the end of the Cold War opened a fundamental--and possibly pre-existing--ontological hole within (over?) U.S. national security policymaking. Without an Other to offer focused, comprehensive threats to the nation, the polity is threatened by internal disorder and indiscipline arising from the collapse of a cohesive Self.<sup>36</sup> In the absence of compelling, coherent, material threats that have the potential to affect equally all citizens of the United States and its allies--something akin to a massive nuclear attack by the Soviet Union--there can be no overarching ontology of security, no shared identity differentiating the national self from threatening others, no consensus on what, if anything, justifies priority attention, no "Them" against which to mobilize "Us." For the moment, it would seem, no single real or constructed problem, short of the alien invasions and cometary impacts depicted in recent films, offers the comprehensive threat of focused danger and total destruction once promised by East-West thermonuclear war.<sup>37</sup>

As I shall argue below, the political and disciplinary impacts of narratives of fear are not dependent simply on "facts," inasmuch as the "facts" are neither simply available nor easily constructed, as Latour might argue.<sup>38</sup> Rather, the power of threats rests as much on what the audience does *not* know as it does on that audience's conviction not only that "the world is a dangerous place" but also that each and every reader or listener is a target of these dangers (a dubious proposition at best). Through lurid description and warning, the postulated threats become larger and more ominous, acquiring a materiality of their own as they are endlessly dissected and analyzed by newspaper pundits, on television, radio and the Internet, in barbershops, cafes and town halls. The result is what Annamarie Oliverio has called "the state of terror," in which the invocation of threats becomes a tool of statecraft, and such invocations become the basis for deployment of tools of social control.<sup>39</sup> The audience is terrorized and made fearful not by the hypothesized terrorists<sup>40</sup> somewhere "out there," but by the tales of fear and danger authored and authorized by the state and sources that are presumed to "know." Reassurance against such fears requires, in turn, a material infrastructure to deliver the necessary "protection,"<sup>41</sup> with the result that counter-terrorism becomes, as it were, a booming business.

## **WORMS, BUGS AND TROJAN HORSES**

Let us examine, then, several efforts to address this ontological gap. To fill it, as I noted above, warnings of incipient threats are constantly recited in journals, newspapers and television reports, in Congressional hearings, on the World Wide Web, and at the White House. Yet, these

stories are, somehow, never quite complete. Often there is a certain poignancy about them. For example, the authors of the 1997 *Quadrennial Defense Review (QDR)* rejoiced that

The security environment between now and 2015 will...likely be marked by the absence of a "global peer competitor" able to challenge the United States militarily around the world as the Soviet Union did during the Cold War. Furthermore, it is likely that no regional power or coalition will amass sufficient conventional military strength in the next 10 to 15 years to defeat our armed forces, once the full military potential of the United States is mobilized and deployed to the region of conflict.<sup>42</sup>

But U.S. military power and dominance are, paradoxically, portrayed as potential weaknesses rather than strengths, inasmuch as enemies, too cunning and cowardly to fight on the field of battle, will nonetheless find other means to attack. The *QDR* warns that

U.S. dominance in the conventional military arena may encourage adversaries to use such asymmetric means [e.g., terrorism and information warfare] to attack our forces and interests overseas and American at home. That is, they are likely to seek advantage over the United States by using unconventional approaches to *circumvent* or *undermine* our strengths while *exploiting* our vulnerabilities (emphasis added).<sup>43</sup>

What are the vulnerabilities before which the *QDR* quails?

"Cyberterror" (sometimes called "information warfare") is one.<sup>44</sup> Of books, reports, studies and conferences on the topic of cyberterror, there is no end. Every day brings another warning that the Internet and World Wide Web are under threat from sources both domestic and foreign, statist and individual. For example, on June 25, 1996, then-Director of Central Intelligence John Deutch, appeared before the Senate Governmental Affairs Committee and warned of

[E]vidence that a number of countries around the world are developing the doctrine, strategies and tools to conduct information attacks.... International terrorist groups clearly have the capability to attack the information infrastructure of the United States, even if they use relatively simple means.... [A] large-scale attack on U.S. computer networks could cripple the nation's energy, transportation, communications, banking, business and military systems, which are all dependent on computers that could be vulnerable to sabotage ranging from break-ins by unauthorized 'hackers' to attacks with explosives.<sup>45</sup>

Apparently, Deutch gave good testimony, for Senator Sam Nunn (D-Georgia), then-Acting Chair of the Committee, responded by asking "Where does this fit in the scale of potential threats?" Deutch (who in print has compared a teenage hacker with a laptop to Carlos the Jackal<sup>46</sup>) proposed that

it was very, very close to the top.... I would say that after the threats from weapons of mass destruction, from rogue states and the proliferation of nuclear, chemical and biological weapons, this would fall right under it.

Nunn, seeing and raising the bet, then observed that "some believed" such attacks could result in "an electronic Pearl Harbor" (not, it must be noted, the much more evocative "electronic Hiroshima").<sup>47</sup>

That the Pearl Harbor metaphor has an iron grip on the intelligence community is clear

from testimony in which National Security Agency Head Air Force Lt. General Kenneth Minihan, appearing before the Senate Governmental Affairs Committee, once again warned that an "electronic Pearl Harbor" launched by a foreign government was highly plausible. At the same hearing, CIA Director George Tenet worried that the "occasional teen-age computer hacker" will surely be followed by those in the employ of "hostile governments." He went on to reveal that

We know with specificity of several nations that are working on developing an information warfare capability....Our electric power grids and our telecommunications networks will be targets of the first order.... An adversary capable of implanting the right virus or accessing the right terminal can cause massive damage.

Committee Chairman Fred Thompson (R-TN), who had received a classified briefing on these threats, later listed China, Russia, Libya, Iraq, Iran and "at least seven others" as the parties engaged in such nefarious activities, although what these countries had so far accomplished, he failed to reveal.<sup>48</sup>

Legion are the tales told of teenagers and others who have "broken into" the sanctum sanctorums of corporate, defense, and public cyberspace. Attackers claim to penetrate domestic and foreign systems with ease, sometimes leaving their graffiti-like marks on Web pages, or causing 911 centers to malfunction. Those attacked claim to have been "penetrated" many times, losing billions of dollars in the process and paying hundreds of millions in "protection" money. Scarcely a day passes without a new report of such hacking, leading Attorney General Janet Reno to warn that "If we aren't vigilant, cybercrime will turn the Internet into the Wild West of the 21st century."<sup>49</sup> According to the *St. Petersburg Times*, however, individual hackers are not the real threat, [Tampa Bay security consultant Winn] Schwartau suggests. Foreign governments and organized terrorist groups are. "The threat is from transnational gangs," he says. "How much damage could be done to the United States online with the backing of \$100-million? A lot. And that's just chump change in the international markets."<sup>50</sup>

Over all of this hangs the "electronic Pearl Harbor," the "bolt from the blue" (literal if you count lightning strikes) which so concerned President Clinton that, in 1996, he appointed a Commission on Critical Infrastructure Protection to study the problem and make recommendations for avoiding disaster. The Committee's report, reflecting the widespread concern about infrastructure vulnerability, claims that

Today, the right command sent over a network to a power generating station's control computer could be just as effective as a backpack full of explosives, and the perpetrator would be harder to identify and apprehend....*The rapid growth of a computer-literate population ensures that increasing millions of people possess the skills necessary to consider such an attack.* The wide adoption of public protocols for system interconnection and the availability of "hacker tool" libraries make their task easier....While the resources needed to conduct a physical attack have not changed much recently, the resources necessary to conduct a cyber attack are now commonplace. A personal computer and a simple telephone connection to an Internet Service Provider anywhere in the world are enough to cause a great deal of harm (emphasis added).<sup>51</sup>

According to the Committee's chair, retired four-star Air Force general Robert Marsh, "it is 'only a matter of time' before critical U.S. computer systems that control the nation's power grid or air traffic control networks face major attack" and the Nation is brought to its knees.<sup>52</sup>

Cyberterror is not the only threat of concern amongst the authorities and in the media; discussion of "bioterror" attacks is widespread, too. On March 12, 1995, a Japanese religious group, Aum Shinrikyo, set off a sarin nerve gas device in a Tokyo subway, killing 12 commuters and injuring thousands. This event is now offered as the archtypal example of "bioterror," even though Aum utilized nerve gas and not biological material (but, see below). In a lengthy article revealing the findings of their investigative research on Aum Shinrikyo's activities, *New York Times* reporters Sheryl WuDunn, Judith Miller and William J. Broad write, somewhat breathlessly that

In repeated germ attacks in the early 1990's [sic], an obscure Japanese cult tried to kill millions of people throughout Tokyo and, a cultist has now testified, at nearby American bases where thousands of service people and their families live.... Hoping to ignite an apocalyptic war, the group sprayed pestilential microbes and germ toxins from rooftops and convoys of trucks.

Although neither Japanese nor American authorities seem to have been aware of these attacks when they were alleged to have taken place, and no one died as a result of them, the journalists claim that

For Washington officials trying to build up the nation's defenses against germ terrorism...the cult's five-year effort to sow terror and death with lethal microbes shows that germ warfare, no longer the sole province of rogue states, is within the reach of extremists with a *scientific bent* (emphasis added).<sup>53</sup>

This last warning has become all too common (and unchallenged). According to a "news advisory" posted several years ago on the Web site of the Henry L. Stimson Center in Washington, DC,

Aum Shinrikyo provided a wake-up call about the need to reassess where the real security threats lie in the post-Cold War era. While the U.S. Congress plans to use billions of dollars for a crash program to defend against sophisticated ballistic missiles, terrorist groups have chosen a more prosaic game plan.<sup>54</sup>

In a recent Heritage Foundation report, "Microbes and Mass Casualties: Defending America against Bioterrorism," author James H. Anderson, Ph.D., cites Congressional testimony by W. Seth Carus, a visiting researcher at the Institute of Strategic Studies at the National Defense University in Washington, DC, and David Kaplan, a writer for *U.S. News and World Report*, to the effect that

Shinrikyo had purchased a 48,000-acre range in Australia to test biological agents on livestock; it sent members to Africa to obtain samples of the lethal Ebola virus; and it built two major biological research centers, one in Tokyo and the other at the base of Mount Fuji. The group attempted at least four separate bioterrorist strikes before its Tokyo nerve gas attack in 1995. In two of the cases, it tried (unsuccessfully) to disseminate biological agents in Tokyo using modified automobiles. It also had planned to attack New York and Washington, D.C.<sup>55</sup>

After so many stories, the Aum Shinrikyo would seem to represent the archetypal bioterrorist threat. Evidently not, for Professor Richard Betts of Princeton University has offered instead the following scenario: "Suppose a secretive radical *Islamic* group launches a biological attack, kills 100,000 people, and announces that it will do the same thing again if its terms are not met?"(emphasis added).<sup>56</sup> Betts does not answer this rhetorical question, but he warns that the American public should not feel too relieved that, as a result of the end of the Cold War, "the danger of nuclear war is off their backs."<sup>57</sup> Today, he warns,

The primary risk is not that enemies might lob some nuclear or chemical weapons at U.S. armored battalions or ships, awful as that would be. Rather, it is that they might attempt to punish the United States by triggering catastrophes in American cities.<sup>58</sup>

His *Foreign Affairs* article is illustrated with photos of soliders in gas masks and an emergency response team in isolation suits conducting a practice exercise in New York. Not to be outdone in bidding up the ante, Dr. John D. Steinbruner of the Brookings Institution writes that, while the influenza epidemic of 1918 killed 20 million people worldwide, "A lethal pathogen that could efficiently spread from one victim to another would be capable of initiating an intensifying cascade of disease that might ultimately threaten the entire world population."<sup>59</sup> Picking up on the growing cacophony, in his speech to the 1998 commencement at the U.S. Naval Academy in Annapolis, President Clinton warned that

Our security is challenged increasingly by nontraditional threats from adversaries both old and new, not only hostile regimes but also terrorist and international criminals who cannot defeat us in traditional theaters of battle but search instead for new ways to attack by exploiting new technologies and the world's increasing openness.

To meet these threats, Clinton then announced the establishment of a position of "National Coordinator for Security, Infrastructure, and Counter-terrorism" within the National Security Council.<sup>60</sup>

## **THE TRUTH IS OUT THERE...ISN'T IT?**

As a result of such repetitive litanies, the inhabitants of this *fin de siecle* world find themselves submerged in an atmosphere of constant threat, subject to the "production of truths" linked to "narratives of fear." In using such language, I do *not* mean to suggest that dangers, whether foreign or domestic, terrorist or state-centered, are not plausible, have never occurred or have somehow gained control of people's lives and destinies. I *do* mean to propose that the fear of things unknown, unseen and unexpected has come to play a central role in the contemporary politics and economics of the United States and much of the rest of the world. Indeed, such narratives of fear play a dual role in the life of American society.

On the one hand, they are critical to the production and reproduction functions of those arms and agencies of government and society that, concerned with both foreign and domestic policing as well as security and corrections, have faced a military and intelligence budget that has been fairly static over the past decade (even as domestic corrections expenditures and prison populations have skyrocketed). A rough estimate of such institutions' share of the United States' GDP would certainly approach \$500 billion; for the world as a whole, more than one trillion.<sup>61</sup>

On the other hand, in a society made increasingly unruly by marketization and consequent social change,<sup>62</sup> narratives of fear provide an efficient, non-interventionary mode of social control and a rationale for the surveillance necessary to maintain discipline--what Stephen Gill has called the "neo-liberal panopticon."<sup>63</sup>

The production of truths and narratives of fear are, consequently, based not only on what *is* known but also and what is *not*; what is *knowable* and what *cannot* be known. These truths and narratives emerge from the relative ease of extrapolation and extension, by so-called experts who "know" of such things, from incidents that *have* taken place and those that, as yet, can only be *imagined*. They play on a public made careless by unanticipated prosperity yet fearful of an uncertain future in which they might lose all. As suggested by a spate of recent films about various catastrophes, moreover, they primed for the worst. Things are reported; speculation is rife; conclusions are drawn. That such conclusions are as often wrong as not (the 1996 Olympic bomber, the Las Vegas anthrax scare), having been drawn from dubious premises and incorrect inferences, does not matter; corrections are rarely issued. The initial impression is what counts, not the causality; the flash and bang draw attention, not the detailed minutiae that follow from long, drawn-out investigations; the imputation of responsibility to mysterious forces is titillating, the role of uninteresting or mentally-impaired individuals is not. And, although a singular event with little or no resemblance to others of which it is said to be an archetype does not (can not) establish a pattern, it does not take much rhetorical repetition to create the impression that a single event, such as the bombing of the World Trade Center, represents only the first of many similar attacks that are bound to happen.

But what if we seek and examine empirical evidence that provides support for these apocalyptic claims? Then, the entire enterprise begins to seem rather more shaky. Surely, if such attacks could be engineered, they would have already taken place (although as conspiracy theorists often warn, the absence of evidence is no cause for complacency). Let us ask, for example, how serious have been the cyber-attacks that have so far taken place? In May 1998, Peter G. Neumann, a "well-known" computer security expert at SRI International testified before the Senate Committee on Governmental Affairs that

Malicious attacks can come from anywhere in the world, via dial-up lines and network connections, and often anonymously [sic!]. Thus far, *there have been relatively few truly serious malicious attacks on computer systems and networking...*, although such activities from both insiders and outsiders appear to be increasing, particularly in financial systems.... The recent attacks on Pentagon systems by the unsophisticated Cloverdale kids were claimed by Deputy SecDef John Hamre to be "the most organized and systematic the Pentagon has seen to date"--but they really indicate only how flimsy Pentagon Internet computer security actually is... (emphasis added).<sup>64</sup>

Reports the *St. Petersburg Times*,

The Department of Defense in 1995 experienced as many as 250,000 hacker attacks, says the General Accounting Office, the investigative arm of the U.S. Congress. That's an average of 685 attacks per day, more than 28 attacks an hour around the clock.... The report estimates six out of 10 of the attacks successfully penetrated at least some portion of the Defense Department's computer networks. *Many attacks were never even detected by the military* (emphasis added).<sup>65</sup>

Disregarding for the moment how it is possible to count attacks that "were never even detected," when the statistics offered here are multiplied by the number of security-linked computer systems around the United States, the result suggests a vast and busy army of subterranean hackers, certainly in excess of 10,000.

A 1997 Carnegie Mellon PhD. dissertation on Internet security, written by John D. Howard, reported that estimates of so-called incidents in 1995 ranged from a low of 1,168 reported to the Computer Emergency Response Team (CERT) to a high of 900 million extrapolated from some of the wilder claims in the open literature. Based on Department of Defense calculations, Howard estimated the total number of actual attacks during the same year *on all systems* to have been between 40,000 and 2.5 million. Based on his own calculations extrapolated from activity at one unidentified site (most likely UC-Berkeley), Howard estimated the total number of incidents in the United States in 1995 to have been in the range of 1,200 to 22,800, with the lower number being more likely.<sup>66</sup> Moreover, recounts the CERT Coordination Center, although the number of reported incidents rose to 2,573 in 1996, it declined to 2,134 in 1997.<sup>67</sup>

Perusal of the "Information Warfare Database," compiled on a Georgetown University-based website (and now, apparently defunct), further reveals that data about most of the list's 150-odd incidents from the past 15 years come from a fairly small number of sources, many of which are in the business of providing electronic "security" and which might therefore have a stake in exaggerating the threat.<sup>68</sup> Howard calculates that the chances of any single computer being penetrated are infinitesimal; he estimates "that a typical Internet domain was involved in no more than around one incident per year....[and] a typical Internet host in around one incident every 45 years."

The CERT/CC records show that some sites and hosts are apparently more attractive because they were involved in many incidents each year. This means that for the average, less attractive, domains and hosts, the probability of being involved in an incident is even lower.... In addition, as shown by this research, many of the Internet incidents are minor and often do not involve successful break-ins.<sup>69</sup>

But aren't there thousands of hackers out there trying to break into secure systems? Perhaps not. In the testimony cited earlier, CIA Director Tenet suggested—without any evident irony—that the greatest vulnerabilities to computer systems arise not from mythical superhackers but, rather, a "disloyal or disgruntled employee." The fact that dealing with the "Y2K" (Year 2000) problem requires reliance on outside contractors who, in the interest of corporate profitability, employ large numbers of potentially-subversive foreigners, also made him fearful.<sup>70</sup>

Finally, Martin Libicki, a professor at the National Defense University, tells the following story:

In the fall of 1994, I was privileged to observe an Information Warfare game sponsored by the Office of the Secretary of Defense. Red, a middle-sized, middle-income nation with a sophisticated electronics industry, had developed an elaborate five-year plan that culminated in an attack on a neighboring country. Blue--the United States--was the neighbor's ally and got wind of Red's plan. The two sides began an extended period of preparation during which each conducted peacetime information warfare and contemplated wartime information warfare. Players on each side retreated to game rooms to decide on moves.

Upon returning from the game rooms, each side presented its strategy. Two troubling tendencies emerged: First, because of the difficulty each side had in determining how the other side's information system was wired, for most of the operations proposed (for example, Blue considered taking down Red's banking system) no one could prove which actions might or might not be successful, or even what "success" in this context meant. Second, conflict was the sound of two hands clapping, but not clapping on each other. Blue saw information warfare as legions of hackers searching out the vulnerabilities of Red's computer systems, which might be exploited by hordes of viruses, worms, logic bombs, or Trojan horses. Red saw information warfare as psychological manipulation through media. Such were the visions in place even before wartime variations on information warfare came into the discussion. Battle was never joined, even by accident.<sup>71</sup>

The truth is, nonetheless, out there. Maybe.

Well, perhaps the evidence for biological terrorism shows it to be a serious, impending threat? Once again, the empirical data seem flimsy. For example, the Stimson Center advisory, cited earlier, bases the credibility of its warnings on two "facts":

1. the formulas for nerve and blister agents are well-known; and
2. the ingredients for these weapons are readily available because they can be used to make legitimate everyday products, such as fertilizers, pharmaceuticals, and pesticides.

(In fact, the advisory is part of a Stimson Center campaign to ratify the Chemical Weapons Treaty, which applies only to states.) If both assertions are correct (and there is no reason to doubt their facticity, although the conclusions to be drawn from them might be questioned), then *anyone* can make sarin and *everyone* is a potential terrorist.

A careful reading of the *New York Times* article DuWunn and her colleagues reveals little evidence to support the authors' claims of near-apocalypse. For example, they report that "Aum's biological arms chief was...once a graduate student in biology at Kyoto University...." In spite of the cult's numerous efforts by to cultivate and release botulin toxin, anthrax and Q fever, none was successful (although several members managed to infect themselves), and the group finally fell back on sarin. In a non-sequitur, Aum's failure is then offered as evidence that "such attacks can be harder to carry out than often portrayed [!] and that...limiting germ access can help thwart terrorists."

A detailed account of the use of biological agents during the 20<sup>th</sup> century, compiled by W. Seth Carus while at the Center for Proliferation Studies of the National Defense University, offers the caveats that

To date, few terrorists have demonstrated an interest in bioterrorism, and fewer still tried to acquire biological agents.... Even in some of the confirmed cases, there is no way to determine the seriousness of the interest in biological agents.... Terrorists have used biological agents, but rarely and with relatively little effect. A review of the cases researched for this study identifies five confirmed instances of terrorist use of biological agents, although there may be others that have never been publicly identified....

According to the FBI, there is only one instance in which a terrorist group operating in the United States [the Rajneeshees, who were trying to gain political control of Antelope,

Oregon in the 1980s] actually employed a chemical or biological agent.<sup>72</sup>

Finally, what are we to make of reports in the *New York Times* that it was only *after* reading *The Cobra Event*, a novel by Richard Preston depicting a "lone terrorist's attack on New York City with a genetically engineered virus," that President Clinton "instructed intelligence experts to evaluate its credibility." The resulting study, and an accompanying "war game," concluded that the United States was woefully unprepared to respond to such an attack (although there is no indication that the credibility of the *threat* itself was assessed, especially inasmuch as such genetic engineering is not something one could do in an ordinary kitchen). Clinton nonetheless issued two new "presidential decision directives," meant "to enhance the country's ability to prevent chemical, biological or cyberweapon attacks...." These followed PDD-39, signed on June 21, 1995, intended to place a high priority on preventing terrorists from acquiring weapons of mass destruction. Subsequently, according to a newspaper report, "More than 40 agencies vied for a piece of the new federal pie, eager for part of the billions of dollars that Congress began appropriating for anti-terrorism programs."<sup>73</sup>

## **PRODUCING TRUTHS AND NARRATIVES OF FEAR**

The somewhat random and anecdotal data presented above leads us to ask: "What do we *really* know?" Let us return for a moment to President Clinton's bedtime reading and its political impacts. Here we see the production of truth and narratives of fear *and* the political economy of danger at work together. The President's concerns are piqued by a novel about nasty diseases, by no means the first on the subject; recall Michael Crichton's *Andromeda Strain* (1969), for example, or, for that matter, Mary Wollstonecraft Shelley's *The Last Man* (1826). Presumably, the President has been informed about "NBC WMD" (nuclear, biological and chemical weapons of mass destruction) by his advisors, and there is certainly no shortage of studies on such weapons.<sup>74</sup> Nevertheless, none of the voluminous reports or extensive briefings offered to him seems to have had the impact of what (based on my reading), when all is said and done, is neither a very compelling or well-written piece of speculative fiction (faction?).<sup>75</sup>

Listening to warnings from various experts, one might think that terrorism is on the rise. Paradoxically, however, the available empirical data suggest that such acts are on the wane even as the number of hoaxes is waxing. At a 1998 Senate hearing on chemical and biological terrorism, for example, FBI Director Louis Freeh testified that the agency had investigated 114 suspected cases

involving preparations for attacks with chemical or biological agents or other weapons of mass destruction...[of which]...approximately 80 percent of them have been hoaxes, and the rest of them have been either resolved [sic] or found to be at least attempts without results.

Furthermore, a study commissioned by Attorney General Janet Reno concluded that terrorism was most likely to be committed *not* by a dedicated group, as is often believed, but by single individuals, whose preparations are the most difficult to detect (the example offered is the "Unabomber," Theodore Kaczynski, although the bomber of the Oklahoma City federal building may also fall into this group).<sup>76</sup> Finally, in *Patterns of Global Terrorism, 1997*, the U.S. Department of State reported that

During 1997 there were 304 acts of international terrorism, eight more than occurred during 1996, but one of the lowest annual totals recorded since 1971. The number of casualties remained large but did not approach the high levels recorded during 1996. In 1997, 221 persons died and 693 were wounded in international terrorist attacks as compared to 314 dead and 2,912 wounded in 1996. Seven US citizens died and 21 were wounded in 1997, as compared with 23 dead and 510 wounded the previous year.<sup>77</sup>

There are several other problematic aspects to these "new" threats that also render them much less dangerous to the country as a whole. First, even if realized as described, they would not affect everyone equally or at the same time; second, they are the product of projection and imagined futures; third, they take no account of motivations. Both cyberterror and biological terrorism would, if realized as described, affect only selected groups and segments of American society, with differential potential impacts that are, to a significant degree, correlated with individuals' economic, cultural and social backgrounds and place of residence. For example, although information warfare could have serious effects on critical parts of the electronic infrastructure, the two-day lapse in pager service around the United States in mid-1998, due to a satellite malfunction, suggests that cyberterror would have its greatest impacts on those most invested in the information economy, not the general public. Terrorist attacks, while seemingly random, are not, and the total number of people killed by those most often described as terrorists over the past three decades is on the order of one to two thousand, many fewer than the number who have died in state-sponsored wars.

In any event, experience suggests that particular cities (Washington, D.C., New York) and buildings (federal courthouses and office buildings and "world trade centers") are the more likely targets. While biological attacks could affect all of the residents of a targeted city, the physical consequences would probably be quite spatially-limited, due to the difficulties of ensuring adequate exposure to everyone. Finally, although "rogue" states might be acquiring weapons of mass destruction and the missiles (or ships and suitcases) to deliver them, they also have good reason to be much more fearful of the United State's overwhelming military and projection power. Awareness of such "facts" might be one reason for the relatively muted public response to the new threats; lack of experience with them could be another.

How can such limited risks be made to seem dangerous for everybody? To answer that question, we need to look more closely at the language used to frame threats, and the role of language and discourse in threat (re)presentation. In the case of "information warfare," this is accomplished by drawing parallels between the imagined danger and Pearl Harbor, thereby evoking a number of common associations (including racist ones): sneak attack, treachery, the War in the Pacific, etc. Through this rhetorical linkage, the perfidy and consequences of an electronic "bolt from the blue" are highlighted, while the actual content of the problem, and the question of whether the Pearl Harbor metaphor is in any way germane to a "cyber attack," are simply ignored. Moreover, the testimony of various author(itie)s also carries a not-so-subtle implication that the United States is fully capable of conducting "cyberwar" against others (while the Gulf War and attack on Yugoslavia illustrate many such capabilities). In this way, policy-makers induce fear by projecting U.S. capabilities onto Others who, it is taken for granted, are hostile and are therefore seeking ways to damage the United States (although, it is then argued, they have no reason to feel that way because the United States has only peaceful and defensive intentions). This is a tactic familiar from the days of nuclear competition with the Soviet

Union.<sup>78</sup>

A second difficulty is that the posited threats, and their consequences, are largely the product of *imagination* and the *market*. For example, on the World Wide Web site about *The Cobra Event*, Richard Preston claims that the book's verisimilitude is based on the "over a hundred interviews with people in government agencies, in the military, and in the scientific community" that he conducted. But he then points out that

[I]n fact, there hasn't been a major bio-terror event in this country yet, and so I had to imagine one--which wasn't too hard, since my sources think that one could occur at any moment, and they are preparing for it.<sup>79</sup>

His model for such an event is, once again, Aum's sarin attack which, as we have already seen, did not involve biological weapons. To further bolster the facticity of Preston's book, the *Cobra Event* Web site includes photographs of smallpox victims, to which are appended lurid subtexts describing the disease and its variants.<sup>80</sup>

In other words, there are facts: Sarin in a Tokyo subway. Toxic substances in any hardware store. The United States heavily dependent on electronic systems. DNA manipulation an everyday practice. Plagues killing tens of millions. Hundreds of thousands of college graduates with degrees in biology and chemistry. And there are "facts" Terrorists, disgruntled employees, and schizophrenics "out there." Sophisticated chemical manipulations undertaken in a kitchen. The United States the focus of envy, fear and hatred. Religious "zealots" who hate and attack us. Worldwide Webs of terrorism. Fragile and easily disrupted infrastructure. The world a dangerous place. And so on.

What we see here is imagination and social construction hard at work--indeed, working overtime--creating texts that are accepted uncritically by both experts and the public but whose plausibility, let alone probability, are not even known, and whose veracity is based on one or two unsuccessful and somewhat mythologized incidents. Annamarie Oliverio calls these "terrorist scripts" (I call them "narratives of fear") and argues that such

texts and narratives are used in the discourses of academic and popular texts from schools, universities, private think tanks...and television.... These stories are internalized, becoming part of a culture's collective memory, symbolism, morality, normative prescriptions as well as models for behavior.<sup>81</sup>

And this leads to the third catch: such texts depend almost entirely on what is known (facts)--for example, that deadly nerve gases can be manufactured from off-the-shelf components--and ignore or downplay what cannot be known ("facts")--why an individual or group might choose to make such stuff and release it in American cities. Richard Betts stumbles over this point without recognizing it:

If the United States is lucky, the various violent groups with grievances against the American government and society will continue to think up schemes using conventional explosives. Bombings or hostage seizures have generally threatened no more than a few hundred lives. *Let us hope that this limitation has been due to a powerful underlying reason, rather than a simple lack of capability*, and that the few exceptions do not become more typical (emphasis added).<sup>82</sup>

Betts never probes more deeply into this hope. (I should note that one of the accused World

Trade Center bombers did admit that he and his colleagues had meant to take down the building and kill thousands; in this instance, we do know about motivations and goals, but only after the event. And, this does not mean that, should a similar attack occur in the future, the same motivation would be behind it.)

The authority of such stories is enhanced by what we might call a "paradox of unknowability." As was the case during the Cold War, the inability to know the actual intentions of Those that are not Oneself--and even "knowing the Self" presents serious difficulties--fosters "worst case analysis" and a focus on the idealized capabilities of the Other. Realist belief and practice constructs a political universe in which states, each motivated by its own worst fears, will maximize material capabilities in order to instill a condition of fear and caution in other states. Worst case analysis further posits such capabilities as being available and applied in a maximal fashion, according to their advertised specifications. This leads, in theory, to the feared outcomes. Error, malfunction, misuse, the fog of war, a change of heart do not figure into such a calculus. The worst comes to pass--at least it does in the imagined scenarios that produce the "truth" of the threatened danger. Fear is the political result.

Worst-case analysis is also applied to non-state actors (not surprisingly, given the historical and epistemological linkages between realism and liberalism<sup>83</sup>). In this instance, it is not that the motives of a specific individual or group are unknowable; any member or informer can provide such information if plied with the appropriate incentives through skillful humint. The problem, so disingenuously pinpointed by Betts is, rather, that no *general* formula about *specific* motivations can be articulated beyond asserting that "violent groups with grievances against the American government and society" exist and "will continue to think up schemes" of attack. Such generalities do not help very much in finding and disarming these groups and, therefore, anything that can be added to the specificity of the threat in order to pinpoint them is deemed useful. Thus, to name "Islamic fundamentalists" as a source of danger specifies particular individuals, who can then be subjected to surveillance, interrogation and arrest.

Paradoxically, confessions of ignorance can also reinforce narratives of fear. While the old cliché has it that "what you don't know can't hurt you," the technique applied in this instance is to naturalize a dangerous world in which unknown or unpredictable sources of injury and death lie waiting around every corner: crime, random violence, carjackings, road rage, drug dealers selling to children, satanic rituals, pornography, identity theft. The result is a move *away* from a grounded assessment of risk and toward equating description with actuarial calculations. This move manifests itself as a form of substate realism--an Hobbesian State of Nature--with anarchy manifesting itself in the home or 'hood and an undomesticated society. The mantra of *The X-Files* becomes the official national bumper sticker. "Trust no one" comes to mean "watch your step," lest you be identified as a malefactor whose behavior is interpreted to mask potentially violent grievances against government and society.

This is not a new technique; it was used throughout the Cold war and, even then, was already long-standing practice. But the question of knowledge is central to the telling of narratives of fear. Inevitably, then, we must turn to Foucault and his arguments about the "production of truth." As Paul Edwards puts it, according to Foucault, "power produces truth," that is, "true knowledge, or a set of techniques and rules for the creation and evaluation of statements as true and false. More simply, power determines what can *count* as true and false."<sup>84</sup>

One result of this form of power/knowledge relation is "the unceasing exchanges of truth, which constitute individual subjects and mold the social body, not just in the abstract realm of theory

but in its materials spaces and practices as well."<sup>85</sup> The veracity of such "truths" is not at issue; indeed, reliable empirical evidence could cut either way (as Betts seems to suggest). Rather it is that such "truths" are part and parcel of, as Robert Cox puts it, the "temporary universalization in thought of a particular power structure, conceived not as domination but as the necessary order of nature."<sup>86</sup>

Does this mean that there is no *empirical, material center* to such truth claims? Or that there is a vast conspiracy afoot to mislead the American public and thereby enrich those engaged in providing security (which would suggest that capitalism itself is a conspiracy)? Not at all. As I have suggested above, many exotic risks appear to be well within the realm of the possible, even if their probabilities are too small to be specified. But the calculation of risks and consequences is best left to actuaries; my concern is with the ways in which certain bodies of knowledge become central to the production of truth. Regardless of whether these "truths" are false consciousness or socially constructed, they have real, material consequences and become integral components of the reproduction of society and its material base. Subsequently, it becomes virtually impossible to undo what has come into being, not for physical or cultural reasons but because the political interests that represent and are represented in those material systems are able to resist discursive deconstruction.

One of the most illuminating examples of this process can be found in the discursive framework of nuclear deterrence, which I will not develop here, except to argue that, with nuclear deterrence, one falsification of deterrence theory would have invalidated it and been the end of the experiment. During the Cold War, the hollow at the core of this system of belief and practice was not to be examined; the truths on which its production and reproduction were based were not open to challenge. Those who sought to expose or unravel the logic of deterrence theory found that they were either marginalized by virtue of their lack of credentials and clearances, or forced to commit to the code of silence as the price of entry into the inner sanctum of atomic truths.

Mary Douglas, an anthropologist working in cultural theory, offers an interesting framework for explaining risk and danger as presented to the body politic that helps to illuminate why social change generates a superfluity of threats. In *Risk and Blame*, a collection of essays, she writes about danger and risk, and the ways in which the latter has come to replace the former, in part because "plain *danger* does not have the aura of science or afford the pretension of a possible precise calculation."<sup>87</sup> The scientization of danger is one more weapon in the "struggle for ideological domination," even though such claims of danger may often be spurious.<sup>88</sup> Furthermore, Douglas argues, the change in the meaning of the word "risk" from one involving probabilistic statements to "danger" is part of a cultural dialogue about accountability, a contest to muster support for one kind of action rather than another. Decisions to invest in more technology, or less, are the result of the cultural dialogue. Decisions to invade, to refuse immigration, to license, to withhold consent, all these responses to claims need support from institutions of law and justice.... The language of risk is reserved as a special lexical register for political talk about...undesirable outcomes. Risk is invoked for a modern-style riposte against abuse of power. The charge of causing risk is a stick to beat authority, to make lazy bureaucrats sit up, to exact restitution for victims.<sup>89</sup>

But accountability can work both ways. Failure to reduce or respond to risk raises public ire, but public authorities may find the invocation of risk a way of demonstrating that they are

accountable.

Douglas also underlines the way in which risk analysis, as it has developed in the industrialized world, is biased toward individual cognition and unable to take into account the peculiarities of institutions and organizations in influencing people's attitudes toward various kinds of risks, yet, she argues, organizations are central in the creation and propagation of danger.<sup>90</sup> She proposes that there are three types of risk-perceiving "organizations"--market-based, bureaucratic, and voluntary--each of which has a particular structure, goals, fears and stories, and each of which acts as a kind of "filter on political perception."<sup>91</sup> As we shall see, Douglas's examination of risk--understood as danger--fits nicely in arguments I make below regarding the growing prominence of the market in domestic and international politics. It is also linked to the struggles of competing political factions within the United States to re-establish their former positions of political authority. Through the production of truth and narratives of fear, each faction can offer material rewards to potential supporters in this struggle.

### **“DANGER, WILL ROBINSON! DANGER! DANGER!”**

The proliferation of fears in contemporary society can be understood, I argue, as a product of domestic economic, political and social change and uncertainty, and the problem of social discipline, rather than anything that might be going on "out there." During the past decade, such changes have fragmented what seemed, during the Cold War, to be a coherent and disciplined sense of American identity (a case of false consciousness if ever there was one).<sup>92</sup> The reasons for this "insecurity dilemma" have to do with the loss of boundaries defining and securing American identity; if our sense of self is insecure, how can we determine what is to be protected or defended against? Some suggest that this fragmentation of identity is an historical and cyclical phenomenon<sup>93</sup>; others blame the rise of consumer capitalism.<sup>94</sup> Whatever the specific cause, the relentless search for new threats around which to construct new security doctrines represents as much an attempt to discipline and remobilize the polity as to protect it from either real or imagined dangers and risks.

But there is more to the proliferation of threats than mere discipline; maintenance of the political economy of danger depends on both struggle in the so-called marketplace of ideas *and* accumulation of resources to continue the struggle. The struggle takes place largely over legitimation of the truths produced. Support for one faction or another is generated through the accumulation of both political and financial resources that maintain not only the material superstructures dedicated to providing assurance and protection against one danger or another but also the intellectual episteme that produces and underwrites the truths.

At this point, therefore, we must retreat from Foucault and take up cultural theory and its ramifications for political economy. Here, Douglas's tripartite framework for explaining how organizations perceive risk and danger, and the ways in which their beliefs and actions are designed so as to legitimate a specific set of truths proves helpful. Below, I show a table that draws from and extends her work. What is particularly useful about Douglas's typology is the way in which it can be used to, first, differentiate between types of threats (truths) and, second, map these differences onto conflicting factions within the U.S. body politic. Although Douglas might not approve of the way in which I have used her typology--especially insofar as her interest is geared toward understanding how groups and organizations account for disasters that have actually befallen them--her framework maps onto the production of truths about threats and

risks in some interesting ways. Using this modified approach, we can also bring more conventional security "threats" and "cultural" threats into the same framework.

**Table 1: A typology of threats & risks**

	<b>Market-based</b>	<b>Bureaucracy-based</b>	<b>Voluntary group-based</b>
Type of threat/risk	Calculating	Cosmic	Cultural
Character of threat	Rational action	Unpredictable forces	Internal subversion
Examples	Rogue states; proliferation; malign economic competition; errant missiles & no defense	Bio- & cyber-terrorists; global criminals & drug smugglers; environmental catastrophes; plagues; comets	Cultural collapse & nihilism wars; foreigners & their languages; cyberporn; sexual transgressions
Latent concern of proponents	To preserve individual freedom to contract	Secure internal structure of authority	Survival of group
Disasters predicted	To magnify competition of leaders	To support group control over individuals	To damp dissidence or clarify factions
Latent cosmic forces	Secret or "illegal" weaponry aimed at the United States	Punitive universe (dangerous world) that may strike out any time and kill or injure large numbers	Global plot or betrayal to undermine traditional hierarchy
Accusation	Leader has lost will to power	Group has lost commitment	Individual treachery or malignant forces
Associated organizations	Republicans; defense industry; conservative pundits, academics & think tanks	Democrats; corrections industry; liberal pundits, academics & think tanks	Cultural conservatives; Christian right; militias; conspiracy theorists

Source for rows 4-7: Mary Douglas, "Muffled Ears," pp. 55-82, in: Mary Douglas, *Risk and Blame--Essays in cultural theory* (London: Routledge, 1992), p. 78; rows 1-3, 8 were devised by the author.

*Cultural threats* are propounded by culturally-conservative, voluntary groups who see them originating with liberals, academic marxists, foreigners (both legal and illegal) and social

deviants--in short, those who have strayed from the "norms" of American tradition. Such individuals are to be found everywhere: in media, political life, the military, Wall Street, the White House, Hollywood, Broadway, etc. These are treasonous agents engaged in "global conspiracies" aimed at undermining "American" social hierarchies and moral strictures, and they mean to change the nation into something quite different from what it was (based on a largely mythical past), and in which religion, tradition, family and freedom are dissed by "Forces of Darkness" (it is no accident that such threats are framed in apocalyptic terms). During the 1990s, this Great Treason has been blamed on President Clinton, a baby-boomer who never served in the military, but whose "individual treachery" is said to be evident in everything he has done (or will do). As William J. Bennett puts it in *The Death of Outrage--Bill Clinton and the Assault on American Ideals*,

In living memory, the chief threats to American democracy have come from without: first, Nazism [sic] and Japanese imperialism, and, later, Soviet communism. But these wars, hot and cold, ended in spectacular American victories. The threats we now face are from within. They are far different, more difficult to detect, more insidious: decadence, cynicism, and boredom. . . . [I]f the arguments made in defense of Bill Clinton become the coin of the public realm, we will have committed an unthinking act of moral and intellectual disarmament.<sup>95</sup>

The consequences of not responding to internal threats will be no less than astronomical, as Reverend Jerry Falwell announced when he warned that comets and meteorites would fall on sinful places such as Disney World and San Francisco.

*Cosmic threats* are propounded by those individuals and bureaucratic organizations most concerned with re-establishing the country's "internal structure of authority." This is accomplished through invocation of the common dangers inherent in a punitive universe (aka, "dangerous world") in which unknown or inexplicable forces may strike from any quarter at any moment. Here, the invocation of uncertain but deadly dangers is meant to restore "group commitment," mobilizing the populace into a single national entity by warning that anyone or everyone could be hurt. Because, however, the probabilities associated with non-human agents are basically incalculable and the motivations of unknown human agents are unfathomable ("let us hope"), eternal vigilance and, indeed, constant surveillance are required.

Finally, *calculated threats* are offered by market-oriented individuals and organizations who hold what is, for the most part, a conventional realist view of the world. States and individuals are calculating, rational actors who see either political or economic gain in acquiring the means of undermining American power. Thus, Chinese acquisition of missile targeting technology and nuclear secrets, the destabilizing behavior of a Slobodan Milosevic, the activities of "rogue" states, the North Korean threat to Alaska and Hawaii, and so on, are all American vulnerabilities to which a weakened leadership has exposed the country. Among the purveyors of these threats, there is a competition to raise the stakes by warning of ever-more serious potential breaches of the Nation's safety without indicting specific parts of the country's body politic (as the cultural conservatives are wont to do) or invoking cosmic punishment (as the bureaucrats seem to be doing). One evident contradiction in proffering calculated threats is that the acquisition of the means of danger by external parties (e.g., China) is blamed on the economic objectives of the bureaucrats who are nevertheless engaged in support of the very

system of enterprise so favored by the market-oriented.

Of course, in politics and its struggles, neat partitioning such as that indicated by this typology does not occur. Neither threats nor proponents are as "pure" as this framework would suggest, and the exigencies of political coalition-building means that alliances develop, back-scratching is frequent, and pork-barrelling ubiquitous. During the Cold War, producers of both calculating and cosmic threats (truths) were often united and dominant, although during parts of the 1950s and 1980s, this coalition came under attack as cultural threats (e.g., McCarthyism) came to seem more menacing. At present, the proponents of market and cultural dangers are allied with one another as part of the effort to drive the Democrats out of the White House, although a good deal of the material resources allocated to the new threats are flowing to the bureaucratic producers of cosmic truths. Still, there is the hope that, by producing narratives of fear, and attributing dangers to flaws in the body politic--weak leaders, national fractures, individual treachery--the material balance can be shifted and support for the calculating-cultural struggle might be mobilized.

### **IGNORE THE MEN BEHIND THE CURTAINS!**

Fears do not emerge from vacuum. As we see in our everyday lives, fears not only motivate certain behaviors, they also leads to material practices that further reinforce those fears and create the material superstructures whose existence becomes proof positive that there is something, somewhere worth fearing. Fear of crime, for example, remains pervasive in the United States in spite of statistics that suggest its decline over the past several years in many of its most serious forms. The rational alien (E.T.) observer might presume that such a decline would result in fewer resources allocated or less attention paid to that problem, yet in the case of crime and criminals, this seems not to be the case (and much the same can be said of national security). How, then, could we account for the decline in reported crimes? It might be that there are simply fewer "criminals," for whatever reason. It might be, as some have proposed, that there are fewer young men in those age groups with the greatest propensity to commit criminal acts (although we are warned to remain fearful for, as the male children of post-World War II baby boomers come of age, crime will resume its relentless increase). Perhaps cops have become more visible or greater numbers of citizens are carrying concealed weapons, making crime that much riskier. It might be, as one currently favored theory has it, that "more criminals are behind bars" and are, therefore, unavailable to engage in criminal behavior. There is certainly some evidence for this in the United States' burgeoning number of prisons and prisoners (1.25 million, up by some 100% during the past few years).

But there is more to fear of crime than fear itself. Fear cannot be allowed to wither, and its reproduction cannot be slowed or halted, lest this also lead to the withering of the system of political economy that has grown up around what is euphemistically called the "corrections industry." One element essential to the reproduction of such fears is reassurance that protection from the threat is available, at the right price, via more police, more prisons, more trials, more surveillance and more personal security "systems." Furthermore, as new technologies and ways of doing things, such as commerce over the Internet, are integrated into society, additional activities can be criminalized, further expanding both the production of particular truths and threats--cyberporn, for example, or "identity theft"--and material production--e.g., web-filtering programs and credit card registries--which comes, of course, with a price.

In the case of weapons of mass destruction, Betts notes simply that “‘Counterproliferation’ has become a cottage industry in the Pentagon and the intelligence community, and many worthwhile initiatives to cope with threats are underway.”<sup>96</sup> Betts' contribution in this regard is to propose a civil defense initiative to remedy U.S. urban vulnerability:

A host of minor measures can increase protection or recovery from biological, nuclear, or chemical effects. Examples are stockpiling or distribution of protective masks; equipment and training for decontamination; standby programs for mass vaccinations and emergency treatment with antibiotics; wider and deeper planning of emergency response procedures; and public education about hasty sheltering and emergency actions to reduce individual vulnerability.<sup>97</sup>

According to Betts, such a program would cost more than \$500 million but less than \$4 billion a year, excluding private initiatives that would find ready markets among a credulous public. And there are entrepreneurs aplenty ready to offer individuals the chance to prepare, too. One such private venture is QuickMask®.

QuickMask® is a Respiratory Protective Escape Device designed to reduce the health risks and mortality rates associated with inhalation of toxic air.... Pocket size and lightweight, QuickMask® is designed to be instantly available at all times. QuickMask® can be carried discretely or stored just about anywhere.... Customers include: U.S. Marines, Pentagon Police Force, Federal Reserve Banks, Department of Justice, Defense Criminal Investigative Service, Nuclear Plant Security Forces, U.S. Law Enforcement Agencies and Fortune 500 Companies.<sup>98</sup>

I do not mean to suggest that Betts is a shill for the "security" or corrections industries; as an academic and sometime policymaker, his role is to "produce the truths" that generate the narratives of fear and foster the demand for the political economy of danger. In doing so, he reaffirms and stabilizes the structures of belief and practice that enhance social control, and legitimates the activities of those who cater to the demands of a fearful public. He's just doing his job.

In other words, the production of narratives of fear and the political economy of danger are not the consequence of error or misperception or intelligence failures, as the security literature might have it. They are part and parcel of the production and reproduction of the sovereign, autonomous nation-state, whose role and authority depend on maintaining the appropriate relationship between, on the one hand, citizen and state and, on the other hand, that state and its counterparts in the international "system." The state is "real," but more in the sense that the "man behind the curtain" was real and could call on the terrors of Oz to discipline Dorothy, her companions and, indeed, the inhabitants of the Emerald City. L. Frank Baum's metaphor was one based in the political economy of the times in which he wrote. For the average Midwestern farmer, fear of the Wicked Witches of East and West served the cause of social discipline by dampening popular opposition to a changing industrial society. The same can be said of the author(itie)s of today's imagined stories (although there is quite a gap between their politics and Baum's).

And, so, it becomes perfectly reasonable for someone like the *New York Times* political pundit William Safire to help keep fear at a fevered pitch, by imagining futures in which the

worst comes to pass. What if, he asks, "rogue states"--North Korea, China, whatever--launch nuclear-armed ballistic missiles at Alaska, Hawaii (Pearl Harbor again!) or mainland cities, or Saddam Hussein, in control of a "weapon of mass destruction on a ship near to United States...is ready to sacrifice Baghdad if you are ready to lose New York?" What then? Safire lauds the findings of a new "Team B" (conveniently forgetting the vastly overstated warnings of the original Team B in 1976 or, for that matter, the Bomber and Missile Gaps), the Congressionally-appointed "Commission to Assess the Ballistic Threat to the United States," whose members are "former high government officials, military officers and scientists of unassailable credibility." Countering the more measured assessments of the CIA, the Commission has warned that such attacks are likely to come sooner rather than later (as they always are). Safire argues, therefore, that

we need to defend ourselves from the likely prospect of surprise nuclear blackmail...[for] if we do not decide now to deploy a rudimentary shield, we run the risk of Iran or North Korea or Libya building or buying the weapon that will enable it to get the drop on us."<sup>99</sup>

Safire never makes clear how such a system might defend New York against Saddam's ship, or what "Iran or North Korea or Libya" will do after they run out of bombs and missiles. No matter. Safire's job is not to answer such objections; his vision of the future is meant to instill fear, mobilize political support for those who advocate such a system, and generate material resources for near-term deployment of ballistic missile defense, a pet project of the cultural conservatives and market-minded realists.<sup>100</sup>

Not long ago, the Clinton Administration gave in to the joint cultural-calculating offensive underway in the U.S. Congress and agreed to support deployment of a limited anti-ballistic missile system designed to meet the very threats invoked by Safire and others. Conveniently, perhaps, this took place at the same time that investigations were coming into public view of supposed Chinese nuclear espionage. The secrets "stolen" by the People's Republic would provide it with the very capabilities needed to render such ballistic missile defense both necessary and ineffectual. In all of the noise and bustle accompanying the publication of the Cox Report, no one seems to recall that, according to nuclear deterrence theory, such capabilities were once thought to reinforce strategic stability and increase security. *Sic transit!*

## Endnotes

1. This article is based on a work in progress, *Minds at Peace? National Security, Narratives of Fear and the Political Economy of Danger*. A version of it was presented at the ISA Convention in Washington, DC, Feb. 16-20, 1999. The project is funded by a Research and Writing Grant from the John D. & Catherine T. MacArthur Foundation and by the Social Sciences Division at UC-Santa Cruz.
2. Interviewed on "The Real C.I.A.: Enemies, Secrets and Spies," broadcast on Showtime Sunday, Nov. 29 at 10 p.m. E.S.T., excerpts at <http://www.nytimes.com/library/national/index-cia.html> (Dec. 10, 1998)
3. John M. Broeder, "Clinton Seeks \$1.1 Billion to Fight Terror," *Los Angeles Times*, Sept. 10, 1996, p. A1.
4. Ronnie D. Lipschutz, "Deep Impacts? or Metaphors and Rhetorics of Doom in Global Politics," Paper prepared for a Symposium on "Metaphors and Politics" at the 22nd annual scientific meeting of the International Society for Political Psychology, Hotel Okura Amsterdam in Amsterdam, The Netherlands, July 18-21, 1999.
5. Sheryl WuDunn, Judith Miller & William J. Broad, "How Japan Germ Terror Alerted World," *New York Times*, May 26, 1998 (nat'l ed.), p. A1.
6. David Campbell, *Writing Security* (Minneapolis: University of Minnesota Press, 1992), p. 1.
7. Bruno Latour & Steve Woolgar, *Laboratory Line--The Construction of Scientific Facts* (Princeton, NJ: Princeton University Press, 1986; original edition, Sage, 1979); and Bruno Latour, *Science in action: how to follow scientists and engineers through society* (Cambridge, Mass. : Harvard University Press, 1987).
8. Annamarie Oliverio, *The State of Terror* (Albany: SUNY Press, 1998).
9. H. Ullman & W. Getler, "Common Sense Defense," *Foreign Policy* 105 (Winter 1996/97):3-20. This is also discussed in my forthcoming book *After Authority--War, Peace and Global Politics in the 21<sup>st</sup> Century* (Albany: SUNY Press, 2000).
10. Gregory Foster, "Interrogating the Future." *Alternatives* 19, #1 (Winter 1994):53-98.
11. R. Chase, E. Hill & P. Kennedy, "The Pivotal States," *Foreign Affairs* 75, #1 (Jan./Feb. 1996): 33-51.
12. N.D. Levin, (ed.), *Prisms & Policy--U.S. Security Strategy after the Cold War* (Santa Monica: RAND, 1994). See, however, the 1997 *Quadrennial Defense Review* and the 1998 *Report by the Secretary of Defense to the President and Congress*.
13. Borrus, M., et al. 1992 *The Highest Stakes: Technology, Economy and Security Policy* (New York: Oxford U. Press).
14. 1. Huntington, S. 1996. *The Clash of Civilizations and the Remaking of World Order* (New York: Simon & Schuster).

15. Iklé, F.C. 1996. "The Second Coming of the Nuclear Age," *Foreign Affairs* 75, #1 (Jan./Feb.):119-28; Sopko, J.F. 1996/97. "The Changing Proliferation Threat," *Foreign Policy* 105 (Winter):21-36.
16. Laqueur, W. 1996. "Postmodern Terrorism," *Foreign Affairs* 75, #5 (Sept./Oct.):24-36.
17. David Campbell discusses the "drug war" in chapter 7 of *Writing Security*. See also Michael Massing, *The Fix* (New York: Simon and Schuster, 1998).
18. Homer-Dixon, T.F. & V. Percival. 1996. "Environmental Scarcity and Violent Conflict," (Washington, D.C.: AAAS).
19. Linden, E. 1996. "The Exploding Cities of the Developing World," *Foreign Affairs* 75, #1 (Jan./Feb.):52-65.
20. Garrett, L. 1996. "The Return of Infectious Disease," *Foreign Affairs* 75, #1 (Jan./Feb.):66-79.
21. Leiken, R. 1996/97. "Controlling the Global Corruption Epidemic," *Foreign Policy* 105 (Winter):55-76.
22. Tyson, P. 1995. "Comet Busters," *Technology Review* 98, #2 (Feb./March):22-31.
23. Manwaring, M. (ed.). 1993. *Gray Area Phenomena--Confronting the New World Disorder* (Boulder: Westview).
24. Kugler, R. 1995. *Toward a Dangerous World* (Santa Monica: RAND).
25. Lind, W.D. 1991. "Defending Western Culture," *Foreign Policy* 84 (Fall):40-50.
26. See the discussion in John Lewis Gaddis, *Strategies of Containment* (Oxford: Oxford University Press, 1983).
27. See Tammy O. Tengs, et al., "Five Hundred Life-Saving Interventions and Their Cost-Effectiveness," *Risk Analysis* 15, #3 (1995):369-90.
28. here is, to be sure, a more populist group of dangers whose intensity seems to wax and wane: child abusers, Satanists, cigarette smokers. I do not address the relationship between populist and authorized dangers in this paper.
29. Ulrich Beck, *Risk Society--Toward a New Modernity* (London: Sage, 1992; trans. by Mark Ritter).
30. Risk analysts have long puzzled over the apparent paradox that individuals are much more ready to take high-consequence, high-probability risks, such as death by auto, over which they can exercise some control, than high-consequence, low-probability ones, such as nuclear power plant accidents to which they do not choose to be exposed; see, e.g., H.W. Lewis, *Technological Risk* (New York: Norton, 1990).

31. Interestingly, a number of the people I have interviewed consider the loss of domestic social cohesion, due to the impacts of globalization, a more serious "threat" than the ones discussed here.
32. Guy Oakes, *The Imaginary War--Civil Defense and American Cold War Culture* (New York: Oxford University Press, 1994).
33. *After Authority*, ch. 6.
34. Ronnie D. Lipschutz, ed., *On Security* (New York: Columbia University Press, 1995); *After Authority*, ch. 4.
35. See, for example, James Der Derian, "The Scriptures of Security," *Mershon International Studies Review* 42, supp. 1 (May 1998):117-22.
36. Ronnie D. Lipschutz, "From 'Culture Wars' to Shooting Wars: Is there Ethnic Conflict in the United States?" Beverly Crawford & Ronnie D. Lipschutz (eds.), *The Myth of "Ethnic Conflict"*, (Berkeley: Institute of Area Studies Press, UC-Berkeley, 1998).
37. As related, for example, in Paul R. Erlich, et. al. *The cold and the dark : the world after nuclear war : the Conference on the Long-Term Worldwide Biological Consequences of Nuclear War* (New York: Norton, 1984).
38. Latour, *Science in Action*.
39. Oliverio, *The State of Terror*.
40. In using the term "terrorist," I could be accused of succumbing to the logic of the threat system; I use the term, however, as a shorthand.
41. Charles Tilly, "War Making and State Making as Organized Crime," pp. 169-91, in: Peter Evans, Dietrich Rueschemeyer & Theda Skocpol (eds.), *Bringing the State Back In* (Cambridge: Cambridge University Press, 1985).
42. The Pentagon, *Quadrennial Defense Review*, "Section II--The Global Security Environment," pp. 2-3, at <http://www.fas.org/man/docs/qdr/sec2.html>.
43. *QDR*, "Section II--The Global Security Environment," p. 2.
44. Often, the terms cyberterror, electronic warfare, and information attacks are used interchangeably although, to the cognescenti, they have different meanings; see, e.g., the web sites cited in notes 49 and 62, below.
45. U.S. Senate 1996. *Hearings on Information Warfare and the Security of the Government's Computer Networks*, Senate Governmental Affairs Committee, June 25, Congressional Quarterly Database. This is reminiscent of warnings between 1920 and 1985 that attacks on sources of strategic raw materials could leave us without military planes *and* refrigerators; see Ronnie D.

Lipschutz, *When Nations Clash* (Ballinger/Harper & Row, 1989).

46. John Deutch, "Terrorism," *Foreign Policy* 108 (Fall 1997):12.

47. U.S. Senate. 1996. Whether the United States already possesses such a capability was not made clear, although a very small filler in the May 10, 1998 *San Francisco Examiner*, from the Associated Press wireservice, reported that the National Security Agency planned to hack into NASA's computer network to see if it were possible to disrupt or halt the latter's launch and operations capabilities.

48. John Diamond, "CIA director warns of intrusion into government computers," Associated Press, June 24, 1998, Associate Press Archive at:  
<http://wire.ap.org/?FRONTID=HOME&SITE=FLOCA>

49. Robert Trigaux, "Computer Security Experts Warn of Hacker Threat," *St. Petersburg Times*, June 18, 1998, at <http://www.infowar.com/> (6/23/98).

50. Trigaux, "Computer Security Experts Warn of Hacker Threat."

51. Report Summary, " *The President's Committee on Critical Infrastructure Protection*, [www.pccip.gov/summary.html](http://www.pccip.gov/summary.html) (July 1, 1998).

52. "Report Summary."

53. WuDunn, Miller & Broad, "How Japan Germ Terror Alerted World."

54. First Anniversary of Tokyo Subway Poison Gas Attack: Is the U.S. Prepared for a Similar Attack?" March 20, 1996; at <http://www.stimson.org/index.html> (May 12, 1998).

55. "First Anniversary."

56. Richard Betts, *Foreign Affairs* (Jan./Feb. 1998), p. 39.

57. Betts, p. 26

58. Betts, p. 30

59. *Foreign Policy* (Winter 1998), p. 88.

60. Thomas W. Lippman, "Clinton Pushes New U.S. Security Focus," *Washington Post*, May 23, 1998, p. A3.

61. The U.S. defense budget is greater than \$250 billion, and expenditures on policing, corrections, and justice in the United States were slightly less than \$100 billion. Surveillance, self-defense and home and business security expenditures are probably also in the range of \$100 billion.

62. Lipschutz, *After Authority*.
63. Stephen Gill, "The Global Panopticon? The Neoliberal State, Economic Life, and Democratic Surveillance," *Alternatives* 2 (1995):1-49.
64. Peter G. Neumann, "Computer-Related Infrastructure Risks for Federal Agencies," written testimony before the Senate Committee on Governmental Affairs, 19 May 1998. <http://www.csl.sri.com/neumann/senate98.html> (July 20, 1998).
65. Trigaux, "Computer Security Experts Warn of Hacker Threat." Emphasis added.
66. John D. Howard, *An Analysis Of Security Incidents On The Internet, 1989 - 1995*, unpublished PhD dissertation, Department of Engineering & Public Policy, Carnegie Mellon University, April 7, 1997, at: <http://www.cert.org/research/JHThesis/index.html> (July 20, 1998).
67. Computer Emergency Response Team Coordination Center, "Statistics 1988-1998," at: [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html) (July 20, 1998).
68. See [www.georgetown.edu/users/samplem/iw/](http://www.georgetown.edu/users/samplem/iw/). (This web site may no longer exist.)
69. Howard, *Analysis of Security*, ch. 14.
70. Diamond, "CIA Head Foresees Better Hackers,"
71. Martin Libicki, "Is There an Elephant?" *What is Information Warfare* (Washington, DC: National Defense University, ACIS Paper 3, August 1995), at: [www.ndu.edu/ndu/inss/actpubs/act003/a003ch01.html](http://www.ndu.edu/ndu/inss/actpubs/act003/a003ch01.html) (June 23, 1998).
72. W. Seth Carus, *Bioterrorism and Biocrimes--The Illicit Use of Biological Agents in the 20<sup>th</sup> Century* (Washington, DC: Center for Counterproliferation Research, National Defense University, Sept. 1998 revision), p. 9.
73. Judith Miller & William J. Broad, "Plan responds to U.S. vulnerability to germ warfare," *San Francisco Examiner*, April 26, 1998 (*NY Times* wireservice), p. A-20.
74. A simple search on the University of California's Melvyl bibliographic data system for the ten years between 1988 and 1998 reveals some 1,100 citations for nuclear, biological and chemical weapons, and 1,300 on terrorism.
75. An excerpt can be found on the Random House web site, at [www.randomhouse.com/features/preston/cobraevent/index.htm](http://www.randomhouse.com/features/preston/cobraevent/index.htm) (April 29, 1998).
76. Tim Weiner, "Reno Says U.S. May Stockpile Medicine for Terrorist Attacks," *New York Times*, April 23, 1998 (nat'l ed), p. A12.
77. U.S. Department of State, *Patterns of Global Terrorism, 1997*, "The Year in Review," April 1998).

78. Lipschutz, *On Security*, p. 12
79. The quote can be found at [www.randomhouse.com/features/preston/cobraevent/index.htm](http://www.randomhouse.com/features/preston/cobraevent/index.htm) (April 29, 1998).
80. Preston's book is about a genetically-altered virus based on smallpox, the common cold and a neurological disorder that literally melts the brain. It has been developed by a secret post-Soviet organization called "The Concern," which has set up a lab in New Jersey. The virus is stolen by an unstable employee, who prepares the stuff in a sealed bedroom near Houston Street in Manhattan. Well, maybe. It is interesting to note that Tom Clancy's latest potboiler, *Rainbow Six*, is also about the running amuck of biotech company employees. As radical environmentalists, they plan to restore Nature by exterminating humanity.
81. Oliviero, *State of Terror*, p. 143.
82. p. 29, emphasis added
83. Nicholas Onuf, *World of Our Making--Rules and Rule in Social Theory and International Relations* (Columbia: University of South Carolina Press, 1989).
84. Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse*, UC-Santa Cruz, PhD dissertation, History of Consciousness, June 1988, p. 32, emphasis in original. The thesis has been published as *The closed world: computers and the politics of discourse in Cold War America*, (Cambridge, Mass. : MIT Press, 1996).
85. Edwards, *The Closed World* (thesis), p. 36.
86. Robert Cox, *Power, Production & World Order* (New York: Columbia University Press, 1987), p.xx.
87. Mary Douglas, "Risk and Justice," pp. 22-37, in: Mary Douglas, *Risk and Blame--Essays in Cultural Theory* (London: Routledge, 1992), p. 25.
88. Mary Douglas, "Risk and Blame," pp. 3-21, in: Mary Douglas, *Risk and Blame* (London: Routledge, 1992), p. 12.
89. Douglas, "Risk and Justice," p. 24.
90. Douglas, "Risk and Blame," pp. 11-12.
91. Mary Douglas, "Muffled Ears," pp. 55-82, in: Mary Douglas, *Risk and Blame* (London: Routledge, 1992), p. 79.
92. Ronnie Lipschutz, "Negotiating the Boundaries of Difference and Security at Millennium's End," pp. 212-28, in: *On Security*.
93. Campbell, *Writing Security*.

- 94 Stephen Crook, Jan Pakulski & Malcolm Waters, *Postmodernization--Change in Advanced Society* (London: Sage, 1992).
95. William J. Bennett, *The Death of Outrage--Bill Clinton and the Assault on American Ideals* (New York: The Free Press, 1998), pp. 130, 132.
96. Betts, p. 27
97. Betts, p. 37
98. The QuickMask web site is at: [www.quickmask.com/index.htm](http://www.quickmask.com/index.htm) (May 13, 1998).
99. William Safire, "CIA failures opening crisis silo," *Santa Cruz County Sentinel*, July 22, 1998 (*NY Times* wireservice), p. A9.
100. For a compendium of such proposals, see "Missile Defense" at the Policy.com web site ([www.policy.com](http://www.policy.com)).