

STATEMENT OF JACK RILEY BEFORE THE LITTLE HOOVER COMMISSION

INTRODUCTION

I have been asked to comment on the state's vulnerability to terrorism. For my purposes, vulnerabilities are defined as organizational, operational or physical weaknesses that, if exploited by an adversary, would cause substantial harm to public health and safety. Also, my analysis of vulnerabilities is confined to public infrastructure, such as water systems, the electrical grid and so forth. So, not only was the analysis that I am talking about completed before the attacks on September 11th, but we did not assess the vulnerability of iconic targets such as the World Trade Center. Finally, we confine our analysis to threat sources that have demonstrated the interest or capacity to exploit such vulnerabilities.

THE TERRORIST THREAT IN CALIFORNIA

Analysis of historical terrorism data reveals some trends, both nationally and within California.

- With the fall of the Berlin Wall came the death of the left-wing ideologies for most groups. This reduction in the role of leftist movements has meant that there are less 'professional' (full-time) terrorists.
- Unlike the left, right-wing ideologies continue to motivate operations and spawn new groups.
- Violent actions are increasingly ideologically centered on idiosyncratic issue-oriented themes.
- Groups operating in California, like those across the nation, are utilizing more 'leaderless resistance' type tactics
- Increasingly, activists are motivated by religious or theological imperatives that are not seen as legitimate to many with modern or post-modern worldviews.
- Sharing similarities with groups acting on religious motivations, there has been an increase in cultic groups, or

those that act based upon a particular individual's charismatic leadership.

- Political activists appear to be attacking less frequently, yet their strikes are increasingly lethal.

These trends notwithstanding, the odds are relatively low that California will experience an act of terrorism **against its critical infrastructure, the cyber elements of critical infrastructure, or the agricultural sector, that results in substantial loss of human life.**

This may seem like an odd or bold assertion in the face of the 9/11 events, but it is based upon a combination of factors, including:

- The historically low rates of major terrorism in the United States and California (the trend or factor which has changed the most),
- The infrequency with which terrorists worldwide have committed acts of terror against these targets (infrastructure and cyber infrastructure) or employed these methods (cyber and agricultural terrorism) (note that public transportation is the single most important exception),
- The relatively low vulnerability that most of the critical entities examined for this study have to terrorism.

Certainly, we must expect terrorism to occur in California within the coming decade. However, evidence indicates that most acts **against infrastructure** are likely to be minor in nature and substantial threats to public health and safety will be few.

While there is cause for optimism in the near future, there are factors that could change the assessment. Indeed, our assessment indicates that the likelihood of conventional terrorism (using explosive devices) against infrastructure targets is low. Similarly, employment of Weapons of Mass Destruction (WMD) is unlikely (the recent anthrax attacks do not have WMD-like effects). Although these weapons have potentially high-consequence effects, terrorist groups are likely to continue to lack the technical sophistication required to deploy them and the reasonably well-developed intelligence networks required monitor them.

Cyber (or computer-based) and agricultural attacks, however, may not be as difficult to employ. Both may be viewed as relatively low risk to the perpetrators, but produce potentially high payoff in terms of consequences and impact. Of the two, cyber attacks may be the most appealing to terrorist groups, as they can be more easily directed against traditional targets, such as specific individuals, facilities or organizations. Agricultural attacks may be less likely because they generally require groups to attack untraditional targets (e.g., animals and crops) or take on new or emerging policy issues, such as genetically modified food.

CALIFORNIA'S MAJOR VULNERABILITIES

For purposes of this work, California's critical infrastructure includes power generation and transmission facilities; oil and gas production and distribution facilities; water treatment and conveyance systems; transportation and distribution systems; highways, railroads and ports; and general and specialized acute care hospitals.

Power Generation and Distribution

Most observers and industry officials interviewed for this project agreed that, under most circumstances, attacks on California's electrical grid would not produce lasting, catastrophic effects. Well-timed attacks that occur at periods of peak demand (either daily or seasonally) could heighten the impact and lengthen the time that effects of an attack are felt. Similarly, attacks on critical nodes could lengthen the time to recovery and restoration of service. One important point is that publicly available documents contain much of the information needed for individuals or groups to determine how to substantially disrupt power delivery.

Oil and Natural Gas Facilities

The analysis revealed that many oil and natural gas installations are not well protected. Indeed, most are exposed, unguarded, easy to attack, and have the potential to cause physical destruction, casualties, and environmental damage. This is particularly true of facilities located near water supplies, urban areas, or other such

locations. Of particular potential concern are attacks on chemical production facilities. Refineries use numerous toxic chemicals and attacks have the potential of releasing them into the atmosphere and water supply. A toxic chemical plume resulting from fire or explosion would likely have a larger impact on public health and safety than a simple fire or explosion at refinery, since the consequences of the latter might largely be confined to the refinery grounds.

Water Facilities

Water facilities such as large dams have relatively low vulnerability to physical destruction because they are engineered to withstand substantial natural disasters, including earthquakes. Smaller dams, reservoirs, and aqueducts are more vulnerable to physical attack. The consequences of such an attack would depend on a number of factors. For example, destruction of key conveyance or pumping systems during a drought could impose significant social costs. Ecological terrorism against the Bay-Delta region would imperil a substantial portion of the state's water supply.

Surface Transportation

Findings indicate that most attacks on surface transportation systems would be relatively uncomplicated to execute. Surface transportation modes, particularly public transportation, are not protected. Terrorists have targeted public transportation in cities such as Paris and London. Transportation routes such as roads and railroad tracks run for miles through unprotected, and in some cases hard-to-reach, areas. Trains and trucks often carry hazardous materials that, if released, could cause substantial disruption and pose serious health hazards.

Health Care Facilities

Like surface transportation nodes, most health care facilities appear to be very vulnerable to terrorism. Most have minimal security, and populations of immobile clients. Nevertheless, there are few examples of terrorists attacking health care facilities. Were such attacks to occur in the future, it is reasonable to assume that they may

be in conjunction with primary attacks on other targets. The purpose of targeting health care facilities may be to impair the ability to respond to the primary attack.

Cyber Infrastructure

Most components of the cyber infrastructure that relate to physical infrastructure were found to have substantial protection measures in place. Most major systems are isolated from larger computer networks and many have multiple layers of firewalls and other conventional protection mechanisms. In interviews, many system administrators reported conducting frequent penetrability tests. Most such tests, however, do not appear to be independently conducted.

Most of the state's critical cyber infrastructure maintains high levels of human oversight and involvement. Staff in charge of operations and monitoring at various facilities report willingness to intervene when cyber indicators provide suspicious information. Most systems for critical cyber infrastructure appear to use custom products instead of commercial off-the-shelf (COTS) software. This approach likely affords additional protection by limiting the systems' vulnerability largely to insiders familiar with these custom products. In contrast, the vulnerabilities of COTS software are more likely to be known by unauthorized users, such as the "hacker" community.

Our conclusion is that most of the vital cyber systems regulating California critical infrastructure are quite secure from terrorist attack. One cautionary note, however, is that we used available sources of information to identify and characterize the critical physical infrastructure of the state. The same information we accessed is available to individuals and terrorist groups, who may use it as a road map for designing cyber disruptions, decide which critical systems to target, and when to target them.

Agriculture

Although agricultural terrorism has rarely been employed, California's human food chain - like that of the rest of the United States - remains vulnerable to attack. Relatively few animal diseases are both zoonotic (transmissible from animals to humans) and highly

virulent in humans. Thus, agricultural terrorism would most likely have consequences for animal stock rather than humans, although this would bring substantial consequences for the state (primarily economic).

Presently, California lacks the capacity to address some of the more serious consequences of agricultural terrorism, particularly:

- Mass slaughter operations and carcass disposal for large animals¹;
- Forensic investigation of disease outbreaks.

In addition, the state generally has few indicator and warning mechanisms at its disposal with respect to animal diseases. A further complication is that it is generally difficult to diagnose many animal diseases, particularly in their early stages. For example, foot-and-mouth disease, a deadly and virulent infection of cloven-hoofed animals, looks strikingly similar to the early stages of bovine vesicular infections. The latter disease is more easily managed and not as devastating.

During our interviews, state animal health officials were unable to offer practical alternatives to the current system of diagnosis and reporting. Many state officials felt that private firms would reject more aggressive and intrusive disease monitoring mechanisms. The officials were concerned about these issues, but felt constrained by the many inherent difficulties in diagnosing disease and the practical realities of monitoring large, private firms.

MITIGATION STRATEGIES

Despite California's low vulnerability to terrorism, there are ways to further reduce that threat. Of particular policy relevance are mitigation strategies that serve dual purposes. That is, it may be difficult to justify expending scarce public resources to protect against rare terrorist events, there is greater justification for

¹ The recent outbreak of foot-and-mouth disease in Europe illustrates the complicated logistics of this task, particularly as the size of the infected or exposed animal population increases.

undertaking steps that will accomplish other important policy objectives and increase preparedness for terrorism as a by-product.

Overarching Mitigation Issues

A number of threat and vulnerability mitigation issues apply to all three domains, infrastructure, cyber, and agriculture. From our analysis of California's infrastructure, including interviews with industry leaders, we have identified four issues that limit the ability to prevent and respond to terrorist incidents:

- Industry fears sharing information with the government or other research bodies related to their perception of the terrorist threat because proprietary information can then be requested by competitors under the Freedom of Information Act or relevant public disclosure statutes.
- Industry may not report incidents because they prefer to limit damage to what has occurred instead of potentially increasing damage by lowering share prices due to the public's perception of increased vulnerability.
- Attacks may also go unreported because of industry concerns that law enforcement investigations will involve collecting and seizing potential evidence that would make it difficult to continue business as usual.
- Industry officials also express concerns about reciprocity in information sharing with government agencies. Specifically, there are industry concerns about providing requested information yet not receiving the level of feedback presumed to be appropriate in return.

Overall, it is clear that California, like most other states, lacks an intelligence system that disseminates threat and vulnerability information to all of the relevant parties. The list of "relevant parties" becomes increasingly complex as utilities are de-regulated and more private companies assume functions formerly handled by public entities. In addition, the difficulty of developing such a threat dissemination network is heightened by the fact that few of the institutions whose participation is desired, including public and animal

health organizations, utility firms, and most private information technology firms, have procedures for handling information that can be regarded as law enforcement intelligence. For example, there is no common requirement or standard for investigating employees' suitability to handle sensitive information.

Industry and private firm representatives that we interviewed repeatedly mentioned the need to protect their competitive advantage and security information. Consequently, many firms were reluctant to share information about their security procedures. An industry working group that could develop recommendations about how to provide private companies with incentives to share security information relevant to terrorism. For example, companies may require legislative protection and indemnification to willing share sensitive security information. Many corporate representatives registered specific concerns about state freedom-of-information requirements and their ability to protect proprietary information under these requirements. In addition, firm representatives expressed concern about liability from disclosing weaknesses and vulnerabilities. Even if overblown, this perception is enough to hamper information sharing for intelligence purposes.

Finally, it is sound policy to periodically re-conduct this type of vulnerability assessment. Terrorist opportunities, tactics, and motivations have changed over the past several decades. Periodic reassessments of vulnerabilities are justified in the face of this changing threat.

Infrastructure Mitigation Strategies

Public Accessibility to Information

For this report, what we regard as highly sensitive information on infrastructure vulnerability was obtained from public websites. State officials must balance the public's right to know with a reasoned effort to keep information useful to terrorists at least minimally protected.

Minimum Security Standards for Infrastructure Facilities

Many infrastructure facilities lack basic protection measures. As state control over utilities is weakened through deregulation and

privatization, state authorities must look for ways to ensure that minimum-security standards are defined and met.

Promote a Private-Public Dialog on Physical Security

Time and again, we heard from private firm representatives that they are reluctant to share information with state authorities. In their view, this would jeopardize their ability to protect what firms regard as sensitive information. Without developing a mechanism to ensure communication and promote trust, it will be impossible to develop a meaningful intelligence and warning network.

Explore Ways to Develop an Intelligence Network

Currently, there is very little information that is shared between state, law enforcement, and private entities on intelligence matters. In our view, this limits the ability to develop adequate terrorism prevention capabilities. The state should explore alternatives for creating an intelligence-sharing community.

Cyber Mitigation Strategies

California's critical cyber infrastructure systems are generally well protected. Nevertheless, there are some steps that need to be considered that will improve prevention and response capabilities.

Increase Intelligence Gathering

State officials should promote ways to routinely collect information on both cyber vulnerabilities and terrorist activities. Suggested areas in the former category include: maintaining real-time network maps of critical cyber infrastructure; conducting routine, independent vulnerability and penetrability assessments; developing insider threat management programs; and promoting rapid damage assessment capabilities. Similar strategies need to be adopted with respect to terrorists, including developing methods for preserving information that might be useful in later criminal investigations.

Attack Adversary Intelligence Gathering

To penetrate cyber infrastructure systems, terrorist groups would need to conduct active intelligence gathering. To thwart these

reconnaissance activities, proactive strategies may be needed, beyond traditional methods, such as firewalls, encryption, passwords, and the like. In particular, a range of denial and deception measures is available, including zone transfers, ping sweeps, trace-routes, port scans, and social engineering, including the transmission of deceptive information.

Assessment Capabilities

A state alliance with industry reporting agencies may be needed to develop up-to-date and reliable assessment of cyber threats and vulnerabilities. Relevant reporting agencies include Computer Emergency Response Teams (CERTS), insurance and computer security companies, and industry trade associations. Such organizations maintain incident databases that have the potential to provide early warning about the continued adequacy of existing cyber protection mechanisms at critical infrastructure facilities.

Agriculture Mitigation Strategies

Our analysis indicates that the California Department of Food and Agriculture (CDFA) generally lacks the capacity to meaningfully monitor agricultural hazards and promote effective strategies for reducing them. Particular issues to address include:

FAD Diagnostician Training

Foreign Animal Diseases (FADs) are rarely encountered and there is evidence that diagnostic abilities in the *U.S.* are declining. FAD diagnostic abilities and general veterinarian science education are the first line of defense against agricultural disasters. Increasing skills in these areas not only protects against terrorism but also contributes to public health and safety.

Preparedness and Response Exercises

Currently, there are critical gaps in even basic knowledge about the state's ability to respond to large agricultural terrorism. A combination of simulations and games is suggested. These simulations should explore issues of resource coordination, carcass disposal, and

managing public reaction to large slaughter operations. Also, case studies of the experiences of other states and countries facing similar challenges, such as the outbreak of "mad cow" and foot and mouth disease in Europe, would prove very informative in determining what preparations may be necessary.

Logistical and Physical Infrastructure

There are limits to how quickly animal diseases can be diagnosed, but those limits can be counteracted somewhat by improving the communication infrastructure. Timely communication about deliberate contamination, for example, may help preserve relevant forensic information.

Insurance and Compensation

A key objective of revising agriculture insurance programs should be to design a system that maximizes producers' incentives to practice adequate bio-security. As it is now, insurance programs are not an effective tool in promoting biosecurity.