### Detection programs and container security is not cost effect in comparison to the low risk of port attack.

Naraphorn J. Haphuriwat University of Wisconsin–Madison Vicki M. Bier University of Wisconsin–Madison, [bier@engr.wisc.edu](mailto:bier@engr.wisc.edu) Henry H. Willis [hwillis@rand.org](mailto:hwillis@rand.org) 1-1-2011 Deterring the Smuggling of Nuclear Weapons in Container Freight Through Detection and Retaliation

http://research.create.usc.edu/cgi/viewcontent.cgi?article=1129&context=published\_papers

However, evaluations of these and similar programs call into question the cost effectiveness of container security measures. The capital and operating costs associated with nuclear detectors demand consideration of the benefits afforded by new detection technologies. However, it is difficult to assess their security benefits because of deep uncertainty about where and when terrorists might attempt to smuggle a nuclear device through ports, and also about how terrorists might adapt or respond to improvements in nuclear detection systems. Thus, cost–benefit analysis of nuclear detection systems must consider the increased detection capability that systems afford, how the anticipated benefits of this capability would change as threat levels increase, and the role that nuclear detection plays in deterring terrorist use of nuclear weapons (National Academies 2009, GAO 2009a).

### The cost of radiation detection equipment is too high to justify

Naraphorn J. Haphuriwat University of Wisconsin–Madison Vicki M. Bier University of Wisconsin–Madison, [bier@engr.wisc.edu](mailto:bier@engr.wisc.edu) Henry H. Willis [hwillis@rand.org](mailto:hwillis@rand.org) 1-1-2011 Deterring the Smuggling of Nuclear Weapons in Container Freight Through Detection and Retaliation

http://research.create.usc.edu/cgi/viewcontent.cgi?article=1129&context=published\_papers

The GAO (GAO 2008) estimates the cost of radiationdetectionequipment sufficient to support 100% containerinspection for the period from 2007 to 2017 tobe in the range of $2.6–$3.8 billion. We use the cost ofASP monitors, estimated by the GAO, as our inspectioncost. Dividing the cost of 100% inspection by thenumber of years in the relevant time period and thenby the number of containers per year yields an inspectioncost in the range of approximately $20–$50 percontainer.

### Deterrence is high enough – 100% container/cargo inspection is not necessary to reduce terrorism.

Naraphorn J. Haphuriwat University of Wisconsin–Madison Vicki M. Bier University of Wisconsin–Madison, [bier@engr.wisc.edu](mailto:bier@engr.wisc.edu) Henry H. Willis [hwillis@rand.org](mailto:hwillis@rand.org) 1-1-2011 Deterring the Smuggling of Nuclear Weapons in Container Freight Through Detection and Retaliation

http://research.create.usc.edu/cgi/viewcontent.cgi?article=1129&context=published\_papers

On the other hand, if the defender can create a credible perception that the attacker faces a serious threat of retaliation after even a failed attack, then deterrence can be achieved by partial inspection. In this case, the defender may need to inspect only a modest percentage of all incoming containers, thereby reducing the overall costs of inspection.

### Terrorist can counter port security programs – they can’t make us safe.

Jonathon P Vesky 2008 Port And Maritime Security

Terrorists can counter new technologies. If the United States deploys sensors at some ports, terrorists might detonate a weapon before it is inspected, or ship it to another port. If foreign ports screened containers before being loaded onto US bound ships, terrorists could infiltrate the ports. Securing the largest ports might lead to terrorists to use smaller ones. Securing every US bound container might lead terrorists to smuggle a weapon in a small boat or airplane. Detecting an HEU bomb is difficult because HEU emits very little radiation. R&D is underway to address this key issue.

### Port security measures are extremely controversial.

David Auerswald (professor of security studies at the National War College) and Colton Campbell Congress and the politics of national seucirty 2012

Another effect of fragmented jurisdiction is delay. With its array of veto points, the legislative process in the House and Senate is inherently complex. The competition and dispersal of authority among committees – and the potential for joint or multiple referrals – further complicates the path that homeland security legislation must follow. Whereas appropriations may be delayed, but will eventually pass, the enactment of authorization bills has not been a given. In 2008, Congress did not pass the annual DHS Authorization Bill, owing largely to the number of committees involved with negotiation (Strohm 2008). In the 109th Congress (2005-2007), chemical security legislation was delayed for months due to jurisdictional posturing between the House Homeland Security and Energy and Commerce Committees. Evidencing the importance of issue framing, bill draftsmenship, and jurisdictional clarity, both committees fought overall referral of the bill, with the Energy and Commerce Committee attempting to redirect the legislation by striking the word “terrorism” from its text. In 2006, the Senate Committees on Finance, Homeland Security, and Governmental Affairs, and Commerce, Science, and Transportation wrestled over a port security bill for months. Ken Nahigian, a counsel for the Commerce, Science, and Transportation committee, observed, “We had almost identical bills for port security coming out of each committee. For 30 straight days we were locked up in a room from 7:00am to 1:00am arguing about jurisdiction” (quoted in Laskow 2009). After four years without a Coast Guard authorization bill – owing largely to disagreements between committees in sequential referral – Congress passed H.R. 3619 on September 28, 2010. Enacted were a number of provisions for Coast Guard modernization and acquisition reform that had been delayed for years (H.R. 3619, 2010). In each case, distributive and informational pressures exacerbated the conflict between committees, extending the normal timeline for homeland security authorizations.

John Mueller the Woody Hayes Chair of National Security Studies at the Mershon Center for International Security Studies and a professor of both political science and dance at The Ohio State University and Mark G Stewart Australian Research Council Professorial Fellow

Professor and Director, Centre for Infrastructure Performance and Reliability

The University of Newcastle, Terror, Security, and Money: Balancing the risks, benefits, and costs of Homeland security 2011

Given that it can be carried out by a single individual or by a very small group, terrorism, like crime, can never be fully extinguished. Therefore, it is, of course, essentially certain that some target somewhere will be struck by terrorists. However, the chance any individual target will be attacked is exceedingly low, perhaps even vanishingly so in almost all cases. Protection measures may effectively reduce this likelihood further by deterring the terrorists or by reducing the target’s vulnerability to attack. But for the overwhelmingly vast number of targets, they do so by nudging that likelihood from near zero to even more nearly zero. There is also a displacement effect, a transfer of risk. Terrorists can choose, and change, their targets, depending on local and immediate circumstances. This process, of course, does not hold in the case of natural disasters: a tornado bearing down on Kansas does not decide to divert to Oklahoma if it finds Kansans too well protected. In stark contrast, if the protection of one target merely causes the terrorist to seek out another from among the near infinite set at hand, it is not clear how society has gained by expending effort and treasure to protect the first. The people who were saved in the first locale are gainers, of course, but their grief is simply transferred to others.

### Increasing port security cannot protect us from terrorism – even if our ports our “secure”, terrorists will just attack somewhere else.

John Mueller the Woody Hayes Chair of National Security Studies at the Mershon Center for International Security Studies and a professor of both political science and dance at The Ohio State University and Mark G Stewart Australian Research Council Professorial Fellow

Professor and Director, Centre for Infrastructure Performance and Reliability

The University of Newcastle, Terror, Security, and Money: Balancing the risks, benefits, and costs of Homeland security 2011

As James Lewis points out arrestingly, there may be parallels in homeland protection measures with the experience with the Maginot line – a symbol for a “mindless defense mentality” as he puts it – that shows that “an inventive opponent will simply go around a massive defense” The experience in Israel and Russia suggests that the opponent need not necessarily be all that inventive to make use of the effect. Because of the massive numbers of lucrative targets presented by any one country , it also seems essentially impossible – indeed quixotic – to protect them enough so that international terrorists are directed in frustration to visit their violence on other countries. Measures that make it sufficiently difficult for outside terrorists to get into the country may conceivably do so, as may policing and intelligence measures within it, but not ones devoted to protection.

John Mueller the Woody Hayes Chair of National Security Studies at the Mershon Center for International Security Studies and a professor of both political science and dance at The Ohio State University and Mark G Stewart Australian Research Council Professorial Fellow

Professor and Director, Centre for Infrastructure Performance and Reliability

The University of Newcastle, Terror, Security, and Money: Balancing the risks, benefits, and costs of Homeland security 2011

An inference deriving from the displacement or risk transfer effect should be specifically pointed out and considered. Building hurricane shelters in one area does not increase the likelihood another place will be struck by the hurricane, but in the case of terrorism, the displacement effect essentially means that any effort to protect or to deter a terrorist attack on a specific potential target means that other targets become more at risk. Obviously, this would be of no concern if all potential targets could be protected, but that is clearly impossible. Protection policy, therefore necessarily requires making choices about what to protect, and this, equally necessarily means that targets left off the protection list become more attractive to the terrorist.

John Mueller the Woody Hayes Chair of National Security Studies at the Mershon Center for International Security Studies and a professor of both political science and dance at The Ohio State University and Mark G Stewart Australian Research Council Professorial Fellow

Professor and Director, Centre for Infrastructure Performance and Reliability

The University of Newcastle, Terror, Security, and Money: Balancing the risks, benefits, and costs of Homeland security 2011

For example, there is a program to protect bridges in the United States, and a list of something like 200 of the most important bridges has been drawn up. There seems to be no evidence terrorists have any particular desire to blow up a bridge, due in part, perhaps, to the fact that it is an exceedingly difficult task under the best of circumstances and that the number of casualties is likely to be much lower than for many other targets. The apparent hope of the protectors in this case is that, after security is improved for all these targets, any terrorists who happen to have bridges on their hit list will become disillusioned. If so, however, they might become inclined to move on to the 201st bridge, or more likely perhaps, to another kind of bridge: the highway overpass, of which there are some 600,000 in the United States. If the terrorists attention is drawn, further, to any one of a wide array of multiple overpass bridge networks, they might be inclined to destroy one of those. The financial and human consequence, not to mention the devastating traffic inconvenience, that could result from such an explosion might well surpass the destructive consequences of one directed at one of those 200 bridges. The issue, then, is: how has society benefited by the protection of the bridges? The cost effectiveness of bridge protection is discussed more fully in chapter 6.

### Port security fails – multiple reasons

Jon D. Haveman is a founding principal of Beacon Economics. He is widely considered to be one of California’s leading experts on the economics of seaports, goods movement, and  international trade policy. Howard J. Shatz Senior Economist at the RAND Corporation.2006 “Protecting the Nation’s Seaports: Balancing Security and Cost” http://www.ppic.org/content/pubs/report/r\_606jhr.pdf

Immediately after the September 11 attacks, the greatest impediment to improving port security was, therefore, the extent to which it had previously been neglected. Although officials are no longer neglecting security, numerous factors make port security planning and implementation a continuing challenge. These include • Volume. An extremely large amount of goods flows through the maritime supply chain. In 2004, America’s ports handled almost 20 million ocean containers. 6 • Intermodality. Goods arrive at and depart from the port not only by ship but by rail and truck. • Jurisdictional conflicts. Federal, state, and local governments all may have oversight over some portion of port activities. In addition, some ports are managed by local or regional port authorities, whereas others are managed by local or state governments or by private entities. • Quantity of stakeholders. Carriers, shippers, logistics firms, producers, labor unions, and others all work at or use the ports and all must be involved in security efforts for these to be effective. • Global nature of industry. Any serious security effort requires international cooperation from foreign governments, foreign port operators, and foreign ship owners. • Time sensitivity. Production has moved to just-in-time processes, with manufacturers relying on steady shipments of inputs. • Public and private involvement. Both sectors are likely to be interested in having the other carry the burden of financing or even planning security efforts.

### No impact to port attack – ports resillient

Jon D. Haveman is a founding principal of Beacon Economics. He is widely considered to be one of California’s leading experts on the economics of seaports, goods movement, and  international trade policy. Howard J. Shatz Senior Economist at the RAND Corporation.2006 “Protecting the Nation’s Seaports: Balancing Security and Cost” http://www.ppic.org/content/pubs/report/r\_606jhr.pdf

In Chapter 2, Edward E. Leamer and Christopher Thornberg argue that the actual costs of an attack on the Los Angeles–Long Beach port complex may not be as high as many fear. For example, if a port is closed, many shippers will reroute their shipments through other ports. In addition, displaced workers will seek alternative employment. As a result, the economy will adjust. Some output will be lost, but it may be so small in magnitude that it will not reveal itself in data that track national or even regional macroeconomic trends. The authors provide examples of other disruptions that might have caused severe economic damage but did not, such as the terrorist attacks of September 11, 2001. Consumer spending fell immediately after the attacks but then rebounded sharply at the end of 2001, growing at an unprecedented, seasonally adjusted annual rate of 7 percent. Likewise, although retail sales fell immediately after the attacks, they returned to trend in November, only two months later. Some sectors did suffer, most notably the airline industry, which had already been in deep trouble before the end of the technology boom in early 2001. But consumer spending actually increased, suggesting that people reallocated the money that they would have spent on airline travel to other forms of consumption. Similarly, the authors argue that other disruptions such as hurricanes, earthquakes, and even labor disputes at seaports did have immediate negative economic effects but that these effects dissipated quickly as the economy adjusted. The message in this is that most such disruptions lead to business being delayed rather than business being cancelled, which in turn results in much less economic harm than would be expected.

### Port security fails

Jon D. Haveman is a founding principal of Beacon Economics. He is widely considered to be one of California’s leading experts on the economics of seaports, goods movement, and  international trade policy. Howard J. Shatz Senior Economist at the RAND Corporation.2006 “Protecting the Nation’s Seaports: Balancing Security and Cost” http://www.ppic.org/content/pubs/report/r\_606jhr.pdf

The issue is not merely that something could be put in a container illicitly for an attack on the port where it is unloaded but that nuclear 14 Flynn (2004), p. 89.12 weapons or radiological material could be inserted, shipped to the United States, moved inland without inspection, and then unloaded into the hands of terrorists. These objects could then be transported for use in major population centers—perhaps better targets than a port complex. Likewise, explosive material could be put in several containers and then detonated at or near port complexes around the same time, leading to a security reaction that could shut down the entire maritime transportation system until officials, and port workers and management, were certain the threat had passed. There is no way to completely inspect all of the millions of containers entering the United States. They are about as large as a fullsize moving van and are often tightly packed. Inspecting each thoroughly would bring commerce to a halt, exactly the kind of reaction that terrorists hope to generate

### No impact to terror attacks

Jon D. Haveman is a founding principal of Beacon Economics. He is widely considered to be one of California’s leading experts on the economics of seaports, goods movement, and  international trade policy. Howard J. Shatz Senior Economist at the RAND Corporation.2006 “Protecting the Nation’s Seaports: Balancing Security and Cost” http://www.ppic.org/content/pubs/report/r\_606jhr.pdf

Furthermore, it is our understanding from interviews with experts, that it is highly unlikely that the physical damage from an attack would be enough to close the combined ports of Los Angeles and Long Beach completely. The size of the port complex and the large amount of excess physical capacity would make it nearly impossible for a conventional attack to stop or even reduce substantially the amount of cargo that currently moves through the ports—as long as authorities intervened to allow displaced shippers to use other parts of the complex. The port might nonetheless be shut down if the dockworkers refused to work or were prevented from working by the government. Such a directive might affect all the ports on one or both coasts. Although the United States is considerably more trade-dependent today than in earlier periods, this potential vulnerability is offset by a number of factors. One is the shift from ship to aircraft for delivery of many high-value, time-sensitive goods, particularly on the export side. Second, countermeasures to a terrorist strike, such as increased inspections of containers, may be more onerous for imports coming from uncertain ports than for exports packaged in the United States. And although a widespread labor action would stop most maritime trade completely, a terrorist strike would only slow trade rather than stop it.

**Efforts should be focused on making sure terrorists don’t acquire weapons, rather than enhancing physical securities**

**de Rugy 2007**

Is Port Security Funding Making Us Safer? Veronique de Rugy Center for international Studies Massachusetts Institute of Technology November 2007 Mercatus Center, George Mason University www.web.mit.edu/cis/pdf/Audit\_11\_07\_derugy.pdf

**A practical strategy rests on three priorities: 1. Stop terrorists from acquiring the fissile material necessary to build a bomb. That’s where we should spend most of our security funds.** No fissile material, no bomb. We can achieve this by keeping close tabs on fissile materials around the world, buying foreign stockpiles, and helping foreign governments protect or destroy their stockpiles.8 **2. Recover nuclear material and devices in the event that they fall into terrorists’ hands**. The U.S. should lead an international effort with cooperation from abroad in tightening security at foreign ports. The effort would assist in funding systems to bolster nuclear detection abilities in foreign countries or place U.S. agents on site in foreign ports. Partnerships with foreign manufacturers and importers to ensure that their shipments are protected against infiltration are probably also a good idea and would reduce the need for screening every cargo shipment. **3. Invest in response and mitigation capabilities. Without knowing where or how the attack will occur, responders can lower some of the expected damage by developing plans for the aftermath of an attack**. For an attack on a port, such plans include evacuating civilians and personnel, plac- ing emergency equipment within easy reach, training first response and medical personnel to handle emergencies and attacks, and developing business continuity strategies to allow the port to get up and running quickly after an attack. Experts also suggest developing pre-positioned equipment for responders and the American population.9 Finally, **economists conclude that direct prevention on-site for things like physical barriers** (e.g., fences**), surveillance equipment** (closed-circuit television), **and access control systems for employees and visitors is not cost effective. Given that direct defenses are only as good as their weakest link, they tend not to be cost effective: one has to protect everything from every possible mode of attack.**

**The chance of terrorist threat to port is low or non-existent**

**Gyngell and Nikolaos 2012**

Security UPgrade for PORTs Jenny Gyngell and Dr Nikolaos Papas (SUPPORT) BMT groups 2012 http://www.bmt.org/?/51/40/2925#ixzz208YTHmAO

Although the European Maritime Safety Agency (AMSA), FRONTEX and EUROPOL all touch upon port security, the biggest drawback is that they have no executive powers and therefore cannot control national operations. Furthermore**, it would seem that the introduction of the ISPS Code, despite costing billions of dollars around the world, is perceived by many in the industry as something that has provided little benefit**. The main issue is the fact that the legislation does not mandate specific security measures and provide the necessary consultation of how to implement them. There is no specification for basic requirements such as fence quality or the frequency of security patrols. Consequently, this lack of detail has led to a situation whereby there are vast differences within the EU in how ISPS Code has been implemented. Whilst some ports have interpreted the ISPS Code requirements for protected facilities in such a way that they require the use of code cards, fences, CCTV and alert systems, other ports believe that a simple yellow line around the terminal boundary is sufficient enough in order to comply. Clearly this is an unsatisfactory state of affairs. Add to this the fact that **the majority of ports see security as a low-priority issue and the challenges are exacerbated. Many ports believe that the chance of a terror threat to their facility is low or** in some cases, **non-existent** and that **matters relating to terrorism are already being dealt with by the police and the military**. Therefore, there is often reluctance by terminal operators to invest money in security measures that do not directly protect their income.

### Trying to secure the ports would be useless- infinite attack targets.

Veronique de Rugy, April 1 2005, American Enterprise Institute for policy research, “What Does Homeland Security Spending Buy?,” http://www.aei.org/files/2005/04/01/20050408\_wp107.pdf

Taking the analysis a step further, the most efficient options to combat terrorism tend to be efforts to detect terrorists themselves or to respond effectively to minimize the damage after an attack has occurred. Spending to defend particular targets is generally less efficient. Both results stem from the fact that there are an almost unlimited number of targets, and the terrorist gets to choose where to attack. For example, suppose there are 100 potential targets, that we could perfectly defend for $20,000 a piece, that the damage from un-defended attack would be $500,000, and that we could mitigate one-tenth the damage from attack by spending $50,000 on first responders. If we knew where the terrorists would attack, we could spend $20,000 to save $500,000, which would be a prudent investment. But if don’t know the target, we would have to spend $2,000,000 to defend all 100 targets, which outweighs the $500,000 in damage. On the other hand, even if we did not know the target, we could spend $50,000 on first responders to reduce the damage by $250,000, which is an efficient tradeoff.

### Individual ports are working in cooperation with the DOD to solve security problems.

Shaun Walker, (writer for PRWeb) May 24, 2012, PRweb, “National Security Boosted As A Critical Louisiana Port Installs NextGeneration Technology,” http://www.prweb.com/pdfdownload/9540171.pdf

The Greater Lafourche Port Commission, in partnership with national security firm Crescent Guardian, Inc., has completed implementation of an advanced video analytics application to accompany its next-generation video surveillance system. This milestone ensures that first responders in Port Fourchon are receiving “as they happen” alerts identified automatically by the surveillance system and can coordinate their response in real time. This level of data sharing and interoperability is unprecedented and will aid in lowering response times and overall situational awareness during real-time events, placing the port’s security among the most advanced in the nation. The Greater Lafourche Port Commission's is committed to continually improving the security and emergency response preparedness of Port Fourchon by building a Maritime Domain Awareness System that allows local, state and federal agencies such as Harbor Police, Lafourche Parish Sheriff's Office, LOOP, Lafourche Parish EOC, Fire Central Dispatchers, GOHSEP, Department of Defense, Customs, and Coast Guard to collaborate effectively and become more proactive. To do this, the port's director of information technology, April Danos, wanted to find a way to take all technologies and disparate data and bring them into one common operating picture that would allow these several agencies to work collaboratively within the same situational awareness platform over multiple networks. Crescent Guardian, Inc., a partner security firm of the port, developed an effective solution by providing advanced software that could run the new surveillance system for Fourchon’s Maritime Domain Awareness System, or GLPC-C4. The cutting-edge software allows the system to send alerts and alarms if anomalous behavior is detected, meaning there are "No Rules" to be written prior to their use—Making it one of the easiest and most effective systems in the industry to install and use. “The Port Commission was pleased to work with CGI to integrate BRS Labs’ video analytics into Port Fourchon’s Video Management System and the GLPC-C4 System,” said Director Danos. The US Department of Defense supported Port Fourchon's efforts by sharing the DoD-developed capabilities of the Knowledge Display and Aggregation System (KDAS) to serve as the basis for the Port's incident command and control system. The use of KDAS provides Port Fourchon with the unique ability to network its system with the DoD in the event of an incident requiring information sharing.

Can’t solve – must fix system internationally

Charles Goslin, Vice President of International Operations for Duos Technologies, 11/12/2008 “Maritime and Port Security” http://www.duostechnologies.com/ DownloadCenter/WP-MaritimeAndPortSecurity

Globally, there are very few uniform standards for point-to-point control of security on containers, cargoes, vessels or crews - a port’s security in one nation remains very much at the mercy of a port’s security, or lack thereof, in another nation. Organized crime is entrenched in many ports 2 , and a large majority of them still do not require background checks on dock workers, crane operators or warehouse employees. Most ports lease large portions of their facility to private terminal operating companies, who are responsible for their own security. The result of this is a “balkanized”, uneven system of port security and operations management as a whole.

The 9/11 terrorist attacks were by far the most destructive terrorist attacks in history—no terrorist act before or since has killed more than a few hundred people—but the tragic event seems increasing to stand as an aberration, not as a harbinger. Accordingly, it may be about time to consider that, as Russell Seitz put it in 2004, “9/11 could join the Trojan Horse and Pearl Harbor among stratagems so uniquely surprising that their very success precludes their repetition,” and accordingly that “al-Qaeda’s best shot may have been exactly that.”15

Indeed, it is not all that clear that al-Qaeda central, now holed up in Pakistan, has done much of anything since 9/11 except issue videos filled with unfulfilled, self-infatuated, and essentially delusional threats—an array of these can be found in Table 1. The tiny group of perhaps 100 or so does appear to have served as something of an inspiration to some Muslim extremists, may have done some training, has contributed a bit to the Taliban’s far larger insurgency in Afghanistan, and may have participated in a few terrorist acts in Pakistan.16

The Wizard of Oz conclusion of the 10-year quest for bin Laden suggests that Glenn Carle got it right in 2008 when he warned: “We must not take fright at the specter our leaders have exaggerated. In fact, we must see jihadists for the small, lethal, disjointed and miserable opponents that they are.” Al-Qaeda “has only a handful of individuals capable of planning, organizing and leading a terrorist organization,” and although they have threatened attacks, “its capabilities are far inferior to its desires.”17

It seems increasingly likely that the reaction to the terrorism attacks of September 11, 2001, was massively disproportionate to the real threat al-Qaeda has ever actually presented either as an international menace or as an inspiration or model to homegrown amateurs. But rare indeed have been such observations as those from the CIA’s Carle noted earlier.

As 9/11 is an extreme outlier among terrorist events, Carle is an extreme outlier among officials. Applying standard techniques and using the extensive data sets about terrorism that have been generated over the last decades, it can be determined that the chances an American will perish at the hands of a terrorist at present rates is 1 in 3.5 million per year—well within the range of what risk analysts hold to be “acceptable risk.32 Yet, despite the importance to responsible policy of seeking to communicate risk and despite the costs of irresponsible fearmongering, just about the only official who has ever openly put the threat presented by terrorism in some sort of context is New York’s Mayor Michael Bloomberg, who in 2007 pointed out that people should “get a life” and that they have a greater chance of being hit by lightning than of being struck by terrorism—an observation that may be a bit off the mark but is roughly sound.33 It might be noted that, despite this outburst, Bloomberg still managed to be re-elected two years later.34

The situation seems scarcely different in Europe and other Western locations. Michael Kenney has interviewed dozens of officials and intelligence agents and analyzed court documents. He finds that, in sharp contrast with the boilerplate characterizations favored by the DHS (to be discussed below) and with the imperatives listed by Dalmia, Islamic militants there are operationally unsophisticated, short on know-how, prone to make mistakes, poor at planning, and limited in their capacity to learn.10 Another study documents the difficulties of network coordination that continually threaten operational unity, trust, cohesion, and the ability to act collectively.11 Moreover, it is not all that clear that even the bombers in Afghanistan and Pakistan, where explosive assemblers and operations managers operate in a permissive environment, are all that competent either. According the Daniel Byman and Christine Fair, half of the suicide bombers in Afghanistan manage to kill only themselves, and bomb-bearing warriors rather frequently blow each up in manly embraces as they are about to set off on their missions.