



Changing Police Responsibilities Related to Global Terrorism

Presented by Dr. Marvin J. Cetron,
President, Forecasting International
NEIA/MCC Summer Conference
Sun Valley, Idaho
June 7, 2007

Sponsored By:



VERSATERM

Page has been left intentionally blank

TABLE OF CONTENTS

| | |
|---|----|
| Acknowledgments..... | 4 |
| Executive Summary..... | 5 |
| Introduction..... | 7 |
| Trends in Terrorism..... | 9 |
| Trends in Policy and Policing..... | 13 |
| Trends in Technology..... | 19 |
| Conclusions..... | 28 |
| Bibliography..... | 31 |
| Appendix A: Identifying Future Terrorist Risks..... | 33 |
| Appendix B: Revolution, flash mobs, and brain chips. A grim vision of the future... | 51 |

ACKNOWLEDGMENTS

Forecasting International is grateful to the following people for their valuable assistance in preparing this report:

John Kapinos, Strategic Planner, Fairfax County Police Department; Past-President of the International Association of Law Enforcement Planners;

Bernard H. Levin, Professor of Psychology at Blue Ridge Community College; Commander, Policy and Planning, Waynesboro (VA) Police Department; Director of Research and Development for the Society of Police Futurists International; and Vice Chairman of the FBI/PFI Futures Working Group;

Wes Rogers, Lieutenant, Communications Manager, Fairfax (VA) County Fire & Rescue Department;

William Tafoya, Professor at the Criminal Justice Department, School of Public Safety & Professional Studies, University of New Haven; Founder of the Society of Police Futurists International; and former FBI Special Agent;

Alan Youngs, Esq., Ret. Division Chief Lakewood PD, former President Society of Police Futurists International, and member FBI Futures Working Group;

Thank you all for your help with this report. Without it, our work would have been much less substantial.

EXECUTIVE SUMMARY

Forecasting International (FI) is one of the world's premier futurist organizations. Although it specializes in trend analysis, FI is skilled in all the qualitative and quantitative methods used in forecasting. Many of them were developed by Dr. Marvin Cetron, the company's founder and a pioneer in the field.

FI began its work on terrorism in 1994, when it managed the 4th Annual Defense Worldwide Combating Terrorism Conference for the Pentagon. Its conference report, *Terror 2000: The Future Face of Terror*, accurately predicted the rise of Muslim extremism as a source of terror, the terrorists' growing taste for mass bloodletting, the use of coordinated attacks on distant targets, and even an assault on the Pentagon using a hijacked airplane (omitted at the request of the State Department.) Since then, FI has often studied terrorist issues for both government and private industry.

In this report, FI examines the future of international terrorism, particularly as it will affect the U.S. market for security-related software and services. Some of its conclusions also apply to conventional police work. Key findings include:

- International terrorism will grow as veterans of the Iraq War return to their native lands, train sympathizers in the tactics of terror, and spread out across the world.
- Among the Western lands, Britain and France (owing to their large Muslim populations) and the United States will be at the greatest risk of attack, in that order. Further attacks on the scale of 9/11 are to be expected in all three countries over the range of five to ten years.
- These attacks will combine mass bloodshed and economic impact. Now that the World Trade Center is gone, Grand Central Station at rush hour would be an obvious target for Manhattan. Coordinated attacks on shopping malls, tourist attractions, casinos, schools, churches and synagogues, and sports events also are possible. For details, see Appendix A, FI's study of potential terrorist targets based on interviews with serving and retired military officers, counterterrorism specialists, futurists, and hospitality executives. (These last were included because hotels and restaurants are particularly soft targets and have proved to be among the favorite targets of terrorists around the world.)
- The federal government will continue to share the cost of terror prevention with states and localities at roughly the current level until the Iraq War winds down and those funds become available for other uses.
- Homeland Security will aid localities in "hardening" potential targets such as power plants and transit systems. These grants will be made on a case-by-case basis, usually as matching funds. Again, this will wait for the end of the Iraq War.

- America will not significantly reduce its commitment to Iraq until a Democratic president takes office after the 2008 election. Republicans in Congress may compel President Bush to begin leaving Iraq in preparation for the election. If so, it will come too late to allow significant new security funding before the transition.
- The Department of Homeland Security has begun to stretch its funds by providing matching grants to train corporate security forces in antiterrorism techniques and to use private security for operations such as guarding major sporting events. It will do much more of this in the future.
- New technologies will continue to change both antiterrorism and more routine police work. Most will be in their early stages of development five years from now, but will advance rapidly over the following decade. These include:
 - Tiny sensors that can be scattered to detect explosives or biological warfare agents in potential target areas;
 - Conversion software that allows investigators to use incompatible databases seamlessly;
 - AI, expert systems, and data mining software that can recognize patterns in intelligence derived from different sources and warn of a terrorist event in preparation;
 - Software that can recognize suspicious activities viewed by networks of surveillance cameras;
 - Facial recognition software, which is being integrated with passive video surveillance systems to identify wanted subjects in a crowd;
 - Computerized training for antiterrorism operations similar to the military's Battlefield 2 "game" simulator.

INTRODUCTION

For nearly half a century, Forecasting International (FI) has conducted an ongoing study of the forces changing our world. We have attempted to understand where those forces would lead in fields ranging from the tourist industry to the stability of nations, and for clients from General Motors to the YMCA to the Central Intelligence Agency and the White House. On the whole, we have been reasonably successful. Not long ago, an industrial association re-examined a forecast FI had prepared for them a decade earlier. They found that of nearly 100 specific predictions in the report, no fewer than 95 percent had proved to be correct.

In 1994, we turned our attention to a new field, the future of terrorism. At the request of SO/LIC, the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, we organized and managed the 4th Annual Defense Worldwide Combating Terrorism Conference. Unlike previous conference managers, whose work had concentrated on the "state of play" in the world of terrorists and the officials charged with thwarting their schemes, FI was asked to anticipate how terrorism would change in the years ahead. Again, our work proved to be gratifyingly accurate.

The common wisdom then held that terrorism was quickly becoming obsolete, as rogue states learned that sponsoring terrorist attacks cost far more than any possible benefit was worth. Sponsorship of the Lockerbie bombing had subjected Libya to an air and arms embargo, a ban on some needed oil equipment, and the loss of financial assets. Iraq, long a patron of terrorism, had finally exhausted the world's patience by invading Kuwait and lost a precedent-setting war to a broad coalition of foreign powers led, but by no means dominated, by the United States. With those lessons in mind, no state would be likely to sponsor future terrorist acts, and without that support terrorism itself would dry up.

Our conference report, titled *Terror 2000: The Future Face of Terror*, presented a different view. Terrorism, yet said, would grow more common, not less so. Future terrorist incidents would not be sponsored by states, but increasingly by Muslim extremists motivated by a bitter hatred of the West in general and America in particular. And it would be designed to cause bloodshed on a level never before seen, even at the cost of the terrorists' own death. At the time, these predictions were so far from the consensus view of terrorism held by experts in the field that even many of the subject specialists participating in the conference rejected them. They were far better accepted by the generalist forecasters that FI had recruited to the study. In the end, they all proved to be correct.

Some specific forecasts anticipated the September 11 attack with startling accuracy. The report foresaw the execution of a second, much more successful, attack on the World Trade Towers. It predicted the accomplishment of simultaneous assaults on widely separated targets. (This capacity also was displayed in the embassy bombings of 1998.) It even foretold the deliberate crash of an airplane into the Pentagon. That last was removed from the report at the request of the State

Department, which feared that it could give terrorists a valuable idea they might not conceive on their own.

Many of the analyses and recommendations originating in *Terror 2000* were adopted with little change in later studies of terrorism. The reports of both the Commission on National Security (the Bremer Commission) in 1998 and the National Commission on Terrorism (the Rudman Commission) in 2000 relied heavily on our work. Even the 9/11 Commission used substantial portions of these three studies, including many that first appeared in the *Terror 2000* report.

Since *Terror 2000*, the future of terrorism has been a continuing interest for Forecasting International. We have carried out a number of studies in this field for both private industry and government clients.

In this study, FI again examine the future of international terrorism. In particular, it sought to anticipate the future work of the Department of Homeland Security. In preparing to meet terrorist threats and to predict how forces such as government policy and new technology would affect the market for security-related computer software, and related services. Particularly with respect to technology, many of the observations made during this study will apply equally to more conventional police work.

This probably is just as well. According to a study conducted by the Rand Corporation in 2002, when the painful lessons of 9/11 were still fresh, only 10 percent of law enforcement agencies in the United States considered their communities to be likely targets of terrorism. Fully half perceived a terrorist attack as being extremely unlikely. A follow-up study published in 2006 found that concern about a possible terrorist attack had grown, but the number of local law enforcement agencies perceiving an attack as "very likely" within five years remained low. To the extent that future antiterrorist technologies and practices can be applied to routine police activities, they are more likely to be accepted and applied frequently enough to maintain skill levels. The country will be safer as a result.

TRENDS IN TERRORISM

At Forecasting International, we see three major changes coming in the years ahead. They will fundamentally alter both the terrorist threat to the United States and the terms on which we must fight the “war” on terror. The terrorists will continue to gain more fighters. They will gain far more destructive weapons. And they will gain the kind of legitimacy that could make them even more difficult to stop.

Terrorist Ranks Are Growing

In deposing the Taliban regime in Afghanistan and depriving Al Qaeda of a safe haven there, the United States struck a major blow against the terrorist movement as it existed five years ago. Yet by failing to follow up on that success effectively, we have squandered much of the benefit that should have been gained from that first step in the counter terrorist war. And by invading Iraq, we have supplied Al Qaeda and its sympathizers with a cause around which to rally their existing forces and recruit new ones. As a result, the terrorist movement is now growing stronger, not weaker.

There is ample evidence to support this belief. Up to 30,000 foreign fighters are believed to have gravitated toward Iraq, where they are now gaining contacts and experience that will serve them well in future campaigns against the United States. In this, Iraq is now serving the function that Afghanistan provided in the 1980s. The war in Iraq is building a skilled and disciplined terrorist cadre that will fan out across the world.

Saudi Arabia even has been forced to build a major program aimed at keeping young men from going to Iraq. The Wahhid, the dominant Muslim sect in that country, is teaching that joining the *jihad* is the Muslim man’s second-greatest duty, after going to Mecca. They must fight in Iraq, then come back and be available to fight for fundamentalist Islam in Saudi Arabia. Thus are terrorist cells built, independent of al Qaeda but firmly committed to its goals and methods.

Similar developments are seen elsewhere. The Madrid railway bombings were carried out by a semi-autonomous terrorist cell based in Morocco whose members cited the invasion of Iraq as one inspiration for their efforts. In Britain, the London subway bombings in 2005 were the work of a small, independent band of British citizens inspired by al Qaeda. In France and Australia, authorities have arrested a number of Western converts to Islam, many of whom are believed to have joined Al Qaeda or associated organizations since the invasion of Afghanistan. A report by French intelligence officials estimated that there were between 30,000 and 50,000 such converts, and by implication potential terrorists, in that country alone.

It is clear that they have considerable sympathy among Europe’s Muslim population. The French riots of October and November 2005 affected at least 20 cities in that country, resulting in 2,888 arrests, and touched off lesser violence in Belgium, Denmark, Greece, the Netherlands, Spain, and even Switzerland.

More such events are all but inevitable. Saudi Arabia funds an extensive network of religious schools, from New York to Pakistan. Saudi authorities have admitted that as much as 10 percent of the curriculum in those schools contains material preaching

hatred of other religions, the West, and the United States. At times, those schools even have coordinated their sermons to deliver consistent anti-Western messages in far-distant locales. In a preliminary study during 2003, Dr. Borik Zadeh, of Battelle Institute, found that mosques in Ohio, London, Frankfurt, and Paris were delivering virtually identical sermons, the key message of which was an endorsement of global war against the West. In Pakistan, where Saudi Arabia's Wahhabi movement supports thousands of *madressas*, the call to jihad is even more enthusiastic. Those schools are recruiting extremists, sending money and fighters to Iraq, and systematically building an extremist cadre that will pursue the battle against the West for generations to come.

They are most dangerous in their target countries: Saudi Arabia, Australia, Europe, and to a much lesser extent the United States which is protected by distance and the much smaller size of its Muslim population. Individuals from Europe and the Middle East are absorbing the extremist creed, going to Iraq and learning to fight, and returning to their own countries. France, Denmark, Saudi Arabia, and too many other lands are now home to revolutionaries with all the rights of citizens. Identifying these home-grown, foreign-trained terrorists will be one of the most difficult tasks for antiterrorist forces in the years ahead.

If the United States is relatively well protected against extremist fighters schooled in the Iraq War, many law enforcement officials fear that it could face a large and dangerous pool of home-grown Muslim terrorists. As the crack cocaine epidemic grew out of control in American cities during the 1980s and '90s, many young men were swept into the drug trade. They became well-armed, street-savvy, and prone to use violence and intimidation as everyday business tools. Many thousands of these street warriors ended up in prison for lengthy terms.

While there, many young African-American inmates have converted to Islam. Some will lead more peaceful, positive lives as a result of this religious experience. Yet many other socially disconnected Muslim converts, very likely including the most violent, may be ripe candidates for the *jihadi* cause. Over the next decade or so, many of these prisoners will complete their terms and be paroled back into a society that offers them little future. Those who do not join terrorist cells out of belief could do so merely to gain a modest income. It is this idea, that potentially thousands of new *jihadis*, experienced with weapons and street combat and with little love for or stake in American society, could soon be out on the streets that so worries law enforcement officials. These hardened foot-soldiers could form an effective home-grown army for Al Qaeda and similar groups.

This does not guarantee that the United States soon will face a problem with native-born terrorists. However, both Britain and Australia have found that a minority of prison converts to Islam do accept the anti-Western creed and the call to *jihad*. It would not take many such recruits to cause major trouble in the years to come.

They Will Gain WMD

At FI, we take it for granted that the elite among tomorrow's terrorists will have more than plastic explosives with which to make their point. They will have nuclear weapons. Dr. Abdul Kadeer Kahn ensured that when he gave Pakistan what most extremists regard as an "Islamic bomb" and then spread the plans far and wide. Although American policy is to pillory Iran as a nuclear threat while ignoring the much worse threat from Pakistan, Islamabad's atomic weapons are in the hands of a fragile government surrounded by extremists. Of the two countries, Pakistan represents by far the greater opportunity for would-be nuclear terrorists. If Muslim extremists cannot lay hands on a stolen weapon from the former Soviet Union, they soon may be able to obtain them from Islamabad or, further into the future, from Tehran.

They Will Gain Legitimacy

There is another alternative, however, and it seems increasingly likely. Rather than obtaining nuclear weapons from a sympathetic government, Al Qaeda or its spin-offs may soon become the government in any of perhaps a dozen countries. Wherever secular government is weak, it might easily be replaced by a much stronger and more virulently anti-American theocracy with leaders drawn straight from the terrorist movement. Candidates for a terrorist take-over include Iran (where the job already is half-done), Iraq, Sudan, Syria, Pakistan, Afghanistan, the "stans" of the former Soviet Union, and perhaps the Gulf states. However, our own choice for "most likely to undergo a religious revolution" is Saudi Arabia, where the royal family has supported the extremist *Wahhabi* sect for some 200 years. At FI, we will not be surprised if Osama bin Laden returns to his homeland and sets up an Islamist government in Riyadh, with dire consequences for the U.S. economy and for national security.

There is precedent for the transformation from terrorist movement to legitimate government. In Russia, the Bolshevik killed the Czar, took over the government, and established a regime that would survive for seven decades and became one of the world's most powerful nations. In Palestine, Yassir Arafat made the transition from guerilla leader to something resembling a senior statesman, only to be replaced by Hamas, which remains an active terrorist organization. On the other side of Jerusalem, the Irgun Svi, Haganah, and Stern Gang were terrorists as bloody as any that Palestine has ever produced; yet they supplied Israel with Prime Ministers, senior politicians, and statesmen for more than 30 years. Bin Laden and his senior advisors can be expected to attempt to enter mainstream politics in much the same way. FI believes they may be successful.

There is ample precedent for this as well among Muslim extremist organizations. In Palestine and other parts of the Middle East, Fatah, Hamas, and Hezbollah provide the kind of social safety net that governments in the region do not. Food, clothing, education, shelter, jobs, and medical assistance all flow from these organizations, bringing them a kind of legitimacy that terrorism, however widely admired, never could. This service, combined with the corruption of the Fatah government, was the primary

reason Palestinians voted Hamas into power, not the organization's intransigent rejection of Israel's existence.

This is not the last time terrorists will ascend to government leadership. At Forecasting International, we see little chance that Iraq will make a successful transition to peaceful democracy. When the United States withdraws its forces, the current unrest is likely to broaden into an all-out civil war between the Sunnis and Shiites. Though the Sunnis are heavily outnumbered they have a near-monopoly on weapons and military experience. In the end, they will recapture control of the country, returning the Ba'ath Party to power.

There is worse to come. Within five years, and probably sooner, Al Qaeda will begin this same transition. Its practical, day-to-day contributions to the lives of ordinary citizens will provide a foundation for future political activities. Unlike any government in the Muslim world, in almost any country bin Laden already has the allegiance of a majority of the population.

If the terrorists do manage to gain control of a functional country, the nature of the game changes radically. When terrorists become the government, all terrorism is state-sponsored. The budget available to fund terrorist activities grows many-fold. The nation's laboratories and scientists become available to develop chemical, biological, and even nuclear weapons for the cause. If the country is Pakistan, where Pervez Musharraf enjoys the support of virtually none of his citizens, nuclear devices already are available. Preventing terrorists from gaining control over those weapons is one of the most pressing necessities now facing the counter terrorist community.

TRENDS IN POLICY AND POLICING

The key to security in an era of terrorism, of course, is not terrorism itself, but our reaction to it. In the next five years, that reaction is likely to develop in three important ways.

Incident prevention and response should be better funded, and whatever funds are available will be better targeted. This does not suggest that there will be a revolution in Washington's priorities. Rather, a new administration, believing that its predecessors were driven by ideology and wishful thinking, will find it politically convenient to demonstrate pragmatic realism by a conspicuous focus on real-world needs.

The trend toward intelligence-guided policing will continue for as long as terrorism remains a concern. This is one lasting lesson of 9/11.

And, with practice and perhaps a bit of luck, much-needed cooperation will grow among local police and other emergency responders, the FBI, and the Department of Homeland Security.

We should point out that these forecasts probably are the weakest in this report, the ones most likely to fail, because they depend on logical decisions by politicians and bureaucrats who are not well known for making them. In this case, we believe that they are well grounded because they are supported by political convenience as well as logical necessity.

Before examining these trends, there is one other factor to be considered. It is the dominant concern of government today, and the one problem that must be resolved before others, no matter how urgent, can be realistically addressed.

The War in Iraq

Even the best-intentioned observers can argue about most aspects of the Iraq war. They can disagree about how well it is going. They can debate our prospects for eventual success; however success is to be defined on any given day. They can weigh the merits and dangers of setting a timetable for withdrawal. Yet there is one fact about which there is no room for debate: The war is enormously expensive, and the high cost of waging it constrains our ability to deal with other priorities. It will continue to do so for as long as we maintain a significant presence in Iraq.

Legislation now before Congress will appropriate \$96 billion to continue funding the wars in Afghanistan and Iraq, and most of that will go toward the war in Iraq. As of the morning of April 3, the Iraq war already had cost some \$413 billion, and the tab was growing by something in the neighborhood of \$200,000 per minute, \$200 million per day. Most estimates hold that the total cost of the war will reach \$1 trillion by the time the U.S. occupation runs its course. A few put the total at \$2 trillion. The president's FY 2008 budget request alone calls for \$141.7 billion in Iraq war funding, plus an extra \$93.4 billion in supplemental funding to cover the excess costs of the war in FY 2007.

In contrast, the total budget requested for the Department of Homeland Security in FY 2008 is just \$46.4 billion, and that is up 8 percent over the previous fiscal year.

Only \$3.2 billion of that will be available for state and local preparedness funding, including \$1 billion devoted to providing compatible radio systems so that first responders can communicate with each other.

Now consider one other number. The federal deficit in FY 2008 will be about \$190 billion, according to the Bush administration, which is widely regarded as being somewhat optimistic about such things--and that omits most of the cost of funding the Iraq War.

In all, the point should be clear. Any cause that requires more federal money, no matter how laudable, will have to wait for it until the United States has significantly reduced its commitment to Iraq. That includes most improvements in homeland security.

Fortunately, for anyone seeking federal funding, the war is increasingly unpopular. Roughly 70 percent of Americans now want to see their troops brought home as soon as possible, an increase of about 40 percent in little more than a year. Although the midterm elections of 2006 were not a single-issue referendum, as many political commentators now contend, next year's presidential election clearly will be shaped largely by events in Iraq. As things stand, almost any Democrat will beat almost any Republican to become the next president of the United States. And any democrat in the White House will believe that he, or she, has a mandate to end the Iraq War. Even before the next president takes office, the government in Baghdad is likely to be told that it must ask the United States to bring its troops home, so that Iraqis can begin to settle their own differences. We can expect spending on the war to begin winding down the day a Democratic president takes office.

In fact, it could happen sooner. In early April, there is a rumor in the "blogosphere" that Congressional Republicans, terrified of facing the 2008 election with the war still gripping the minds of voters, have set a deadline for President Bush's troop "surge" in Iraq. If there has been no conspicuous reduction in violence by August, according to this rumor, even the president's staunchest supporters will vote to begin reducing troop levels in Iraq. If this is true, the tide of federal dollars flowing toward the war would begin to ebb even before the presidential election. However, with the 2008 budget already in process there would be little opportunity to channel that savings toward other purposes. No matter what happens in the immediate future, that will be a task for the next president.

Trends in Funding

The end of the Iraq War does not guarantee a flood of new funding for the Department of Homeland Security, or for other aspects of the antiterrorist cause. Many other pressing needs will compete for whatever money does become available, including the need to balance the federal budget.

If the current administration in Washington is correct, American troops returning from Iraq will be followed by a host of terrorists. If so, the cause of homeland security will be able to find many uses for whatever new funding eventually becomes available. On balance, they are likely to receive at least some of the money they need—especially if terrorists again strike within the United States. Even during the Iraq War, the budget for the Department of Homeland Security has grown yearly, by 6 percent in FY 2007 and 8 percent in the request for FY 2008. This has not been enough to cover anywhere near all the programs that need money, but it sets the course for future budgets. A Democratic president, eager to show himself strong on defense, but more focused on national safety than his predecessor, might reasonably devote useful portions of the money saved from Iraq to security improvements at home.

Several specific programs are likely to see more money in future budgets. These include high-profile needs, such as pilot programs to screen all baggage on airliners, development of radiation detectors to prevent the smuggling of nuclear devices into the United States, and enhanced screening programs—preferably based in foreign ports—to ensure the safety of cargoes shipped to the U.S. However, many less conspicuous efforts also should benefit from improved funding. With the aid of federal money, we particularly expect to see more emergency response training and exercises filtering down to ever smaller communities in the years ahead. These will help to ensure efficient and effective responses to natural disasters as well as to terrorist incidents.

Alan Youngs, former President Society of Police Futurists International, and member FBI Futures Working Group, points to another funding trend. "In the future," he says, "more and more law enforcement agencies will form private-public partnerships. Homeland Security will tie grant monies to the existence of these partnerships and the leveraging of resources. Private security out numbers law enforcement three to one. It makes sense economically to utilize their resources for the security of the homeland." For example, it costs \$43 per man-hour for municipal police to provide security at a major sporting event or other public gathering. The same thing can be done by private security guards for \$28 per hour. The state of Colorado in particular is making extensive use of private security for these operations. Many more such activities will be funded in the next Homeland Security budget and in future years.

However, given present funding constraints, it is likely to be FY 2009, or even 2010, before much more help from Washington arrive in American communities. Until then, state and municipal governments will have to make do with approximately the resources they already have.

Trends in Policing

The 1980s and '90s were the decades of community policing, when big-city departments attempted to build closer ties with the citizens they attempt to serve. The idea was that residents who felt a shared ownership of the community with local law enforcement would be less likely to get into trouble and much more likely to cooperate with the police when problems did arise. This "back-to-the-future" policy was an attempt to restore the civil order of the days when everyone knew the cop on the beat, and it worked rather well.

However, like so many other aspects of society, it changed with the terrorist attacks of 9/11. Suddenly, the Muslim community, a growing part of many American cities, was a potential enemy, and Muslims viewed their neighbors and, increasingly, local law enforcement as possible threats to their own safety. This unexpected and unhealthy change was made worse by federal policies that regarded peaceful Muslims much as an earlier generation had viewed Japanese-Americans during World War II.

In the minds of law enforcement leaders and theorists, community policing was never abandoned, but much of their attention shifted to another catchphrase: "intelligence-driven policing." Here the idea was to use information technology to identify trouble, preferably while it was still in the planning, and to investigate crimes and apprehend both terrorists and common criminals when anticipation was not enough. We will look much more closely at what new powers this will make available in the section about technology trends just ahead. For the moment, it is enough to understand that information-based policing will continue to be a major focus of development and training well into the future.

There is one other trend that may tend to work against community policing and other effective policies from the past. This is the rapid retirement of older police officers over the next few years. As the Baby Boom generation of officers is lost, they will take with them their knowledge of valuable contacts within the community, useful procedures they have developed ad hoc, and especially the memory of past cases. We have already seen a similar loss in the intelligence community, where younger personnel have great skill and comfort with signals intelligence and the use of satellite imagery but have lost the understanding of human intelligence. "HUMINT"—developing personal contacts in the target area, old-fashioned spying, and just "shmoozing" with the locals—was necessary to put their intercepts into a useful context, and its loss has made contemporary intelligence work much less effective. We may see a similar degradation of police work as older officers retire and institutional memory is lost.

Trends in Professional Relations

After 9/11, the federal government put considerable effort into figuring out what had gone wrong in the run-up to the terrorist attacks. Why had the nation's law enforcement and intelligence agencies not detected the plot in advance? Why had they not been able to prevent a devastating assault that, by its magnitude and nature, must inevitably have scattered evidence of its existence far and wide long before it scattered debris across southern Manhattan?

The answer turned out to be dismayingly simple. Much of the evidence had been detected, often in time to prevent an attack. Yet no one agency had enough of it to assemble the data into a recognizable picture of what was to come, and those who had one part of the puzzle never shared their information with those who had others. This was the result of more than bureaucratic rivalry. The FBI and CIA in particular were forbidden to share information except in extremely restricted circumstances, for fear of invading the privacy of innocent American citizens. The CIA could not even gather information within the United States, owing to the 1950s-era fear that the agency could slowly mutate into some kind of secret police. They certainly were not about to give classified data to local law enforcement, which might have been in a position to act against plotters hiding within their communities.

Since 9/11, many of the restrictions on information collection and sharing have been lifted. Yet, in order to balance the new powers of information gathering granted to the FBI within the United States, other restrictions have been created. The CIA and FBI have been empowered to share information under much broader circumstances than was formerly possible, but FBI policy prevents some of the Bureau's own departments from sharing information with others. At least temporarily, these restrictions are likely to grow tighter, not less so, in the wake of reports that agents have been widely ignoring both legal restrictions and Bureau policy in using antiterrorist powers to obtain information about Americans who have never been suspected of connections to terrorism.

Yet other information-sharing programs are working well. One good example is the National Capitol Regional Intelligence Center (NCRIC) in the Washington, D.C., area. NCRIC was established to meet the post-9/11 need for regional information exchange, using many of the structures and practices developed by the Sniper Task-Force in response to the October 2002 attacks by John Allen Muhammad and Lee Boyd Malvo. This center is staffed by law enforcement intelligence personnel from various federal agencies, state police from Virginia and Maryland, and local law enforcement agencies throughout the region. The state and local agents assigned to the Center receive federal security clearances so they have access to raw intelligence from federal sources. Those agents keep track of intelligence data and, when needed, provide unclassified versions to their agencies. Even classified information may be passed along on a need-to-know basis. Similar organizations, known as Fusion Centers, have been established in other parts of the country. We expect them to play a greater role in

antiterrorist activities, and perhaps even in conventional police work, five years from now than they do today.

In addition to sharing information, many agencies at the state, regional, and local levels are beginning to integrate resources, procedures, and training to a much greater degree than in the past. Joint training and resource procurement between police, fire, and EMS services is common in many jurisdictions. In an emergency, this should allow them to function together much better than the NYPD and FDNY were able to do on 9/11. Given the threats of bioterrorism and pandemic flu, many local and state health departments also are being integrated into the emergency management protocol.

Many futurists are predicting that within 20 years or so, many cash-strapped local jurisdictions will cease to maintain stand-alone police, fire, EMS, and health departments. Most will administratively merge these agencies into one super “public safety agency,” which will deal with a wide range of actual or potential threats. Divisions within these agencies will focus on particular issues, such as crime control and fire suppression. But many of their personnel will be deployed as needed to deal with threats from terrorism, natural disasters, or pandemic disease. The emphasis will be on the agility and flexibility of public agencies to respond to and mitigate a broad spectrum of threats.

There will, of course, be a price for this kind of flexibility. Cross-training emergency personnel in more than one specialty is expensive. Some states already encourage firefighters and emergency medical technicians to learn each others’ skills, but EMT training is paid for by the student, not the community. Adding basic police work to the mix will be even more costly. However, giving all first responders a kind of generalized disaster-preparedness training should be relatively affordable. It would go a long way toward achieving the kind of flexibility that forecasters tend to believe will be required in the years ahead. That much, at least, seems likely to be accomplished.

TRENDS IN TECHNOLOGY

At the moment, at least three major technological revolutions are under way and several lesser ones as well. Computers are growing so much more powerful that the change is not merely quantitative, but qualitative. Biotechnology is giving us control over life itself. Nanotechnology promises unprecedented control over atoms and molecules, with a host of practical inventions as a result. From these will come tiny, ubiquitous new sensors capable of detecting and reporting on anything, from the state of your cardiac arteries to the presence of explosive traces in the air at your local shopping mall. Thanks to our growing understanding of physics, we also are on the verge of a revolution in energetics, the technology of things that go bang. All of these revolutions will change the practice and aims of policing, especially as it applies to antiterrorist activities.

For a look at what this eventually will mean, let us step a bit farther into the future than we are now concerned with. Then we can come back to the next few years and see how the immediate future will approach, and set the stage for, this more distant vision.

The date is June 27, 2023. ADES, the Automated Data Evaluation System, reports that it has picked up a possible threat. Anyone with secrets to keep and a few thousand dollars to spend on security now scrambles telephone calls and Internet messages using cryptography that for any practical purposes cannot be broken. Yet someone has been careless. Among the billions of communications that ADES has monitored in real time over the past two weeks, five have mentioned Washington in connection with other words that of themselves are innocuous enough but when taken together suggest a disturbing pattern. Among them were “device,” “case,” “monument,” “tower,” “crowds,” “July 4,” and “glorious.” There also was a partial phrase that in English would have sounded like “world tr...” Could the speaker have been about to say “World Trade Center?” We will never be sure; he censored himself before completing the phrase. Yet it would have ended the sentence in which he used the word “glorious.”

Not even ADES would have identified a pattern in this, except that the four telephone conversations occurred in Moroccan Arabic, and each was placed between Jordan and Belgium. The voices all triggered subroutines that reliably detect strong emotions, and one was identified with 92 percent probability as belonging to a minor terrorist suspect living in Amsterdam. Any of these signals would have flagged the conversations for more scrutiny.

In that context, the fifth message became distinctly troubling. Also in Arabic, it had gone by e-mail from Belgium to Florida immediately after the last phone call in the series.

To ADES, it all suggested that a terrorist attack might be planned for the Washington, D.C., on July 4, little more than a week away. The target is almost surely one of the city's many monuments or the crowd that will surround it on the holiday.

Notification from ADES is relayed automatically from the NSA to the CIA. The analyst who receives the report is concerned about the pattern the computer has noted but is not yet convinced. Targeted information retrieval and search "bots" assist the analyst to mine the Agency's extensive data stores as well as piggy-backing on public domain search agents (e.g., GOOGLE, MSN Search, and Yahoo Search.) These efforts turn up additional supporting information.

An hour with evaluation support software and online consultation with two colleagues listed in the Agency's special-knowledge directory provides a firm, defensible train of reasoning. It is time to take action.

First he consults his superiors, convincing them that the danger is real. Then he phones colleagues at the FBI and Homeland Security. They share their suspicions with NCRIC, and the Capitol police department is swiftly brought into the picture. Over the next two days, an ad hoc incident team makes plans and commits the necessary resources. Then they wait.

At 9:15 on the morning of July 4, the nanotechnology sensors scattered around the Washington Monument pick up a chemical trace and relay a report, from each one eighth-inch long unit to all of the others near enough to be within range, until the message arrives at the incident command center. More sensors quickly chime in. They have detected an explosive more than 1,000 times as powerful as TNT. The day will soon come when such sensors protect all public areas routinely, but for the moment they remain too costly for any but the most sensitive areas and accessible sites. Most have been deployed in the District.

Once the subject has been detected, the climax arrives quickly. The sensors have relayed not only the presence of the explosive but their own GPS location. Armed with that information, agents in the area track the suspect's path and identify and capture her with little difficulty. A few minutes later, her contact in Brussels is taken into custody.

Examination of the terrorist's attaché case finds a radio detonator and 12 pounds of explosive equivalent to half a kiloton of TNT. This is what the analyst forecast. In recent years, bombs of this kind have become the weapon of choice for well-equipped terrorists bent on mass destruction.

Searching the terrorist brings a nasty surprise. In one of her pockets is an aerosol container that holds just over an ounce of white powder. The powder turns out to be a weaponized version of the avian flu virus that caused a global epidemic ten years earlier. This strain has been genetically modified to resist vaccines and to be passed even more easily

among human victims. If the captive had chosen to spray the virus around while delivering the bomb rather than saving it for later use, it would have started an epidemic that could have killed millions when Fourth of July visitors returned to their homes around the country.

It seems that even this small band of terrorists has access to skills more often found in a larger organization. Either the cell's members are more sophisticated than most local groups, or they are better connected to international actors than anyone realized.

The long process of tracing their contacts begins.

Some of the technologies in this scenario may seem unlikely to be available in the near future, if at all. The massive computing power and—especially—the artificial intelligence required by a program like ADES sound more like science fiction than fact. So do nanotech sensors, super-explosives, and bioengineered pathogens that could be available to small terrorist cells. Yet these technologies, or their immediate precursors, are under development today.

These innovations, and no doubt others as well, will transform the world in the next twenty years. In the process, they will change the practice of information-based policing in important ways. Some will make data collection and evaluation more efficient, more likely to give an accurate picture of potential adversaries, and more able to detect nascent threats before they can be put into practice. Others will make it almost impossible to gather some forms of data that today are routinely accessible.

At the same time, these technologies, and others, will make extraordinarily powerful weapons available to just about any country, corporation, or small-scale actor that cares to have them. And some will make it nearly impossible to figure out who launched a devastating attack, so no credible threat of retaliation can be made.

That will raise the stakes for American police and antiterrorism services to horrifying new levels. In a world where highly lethal, potentially anonymous weapons can be obtained by almost anyone who wants them, the only effective defense is to detect a pending attack and intervene before it can be carried out. That requires constant, global vigilance down to the individual level. A single terrorist plot, overlooked, could result not in hundreds or thousands of deaths, but in many hundreds of thousands.

Trends in Nanotech

If it's most ardent proponents are correct, nanotechnology in the long run will do more to change our world than all of the other techno-revolutions combined. In the strictest sense, nanotechnology is the construction of tiny machines, one atom at a time; each placed exactly where it is needed to build tiny motors, gears, and other mechanical parts. The Holy Grail of nanotechnology is the "assembler," a molecule-sized robot that

can replicate itself until enough of its kind is available and then begin turning out ... anything.

The future world of pure nanotechnology is a miraculous place in which machines that can be seen only with the most powerful microscopes attend to our every need. Cancer has disappeared, because nanomedics course through our bloodstreams, recognizing cancerous cells and destroying them the moment they appear. Traditional manufacturing and pollution are the stuff of history. Nanotech assemblers build our cars, homes, and other artifacts; just drop some properly programmed assemblers into a vat of raw materials, and stand back as a skyscraper appears to grow spontaneously toward the clouds.

For better or worse, this kind of nanotechnology remains no more than a dream that may never be realized. However, less ambitious forms of nanotechnology already are beginning to generate viable products. For example, the switches that set off airbags in an automobile crash are made by etching the accelerometer and electronics onto a silicon chip in the same way that computer chips are made. So are “digital micromirror devices,” the chips that create the image in Digital Light Processor (DLP) rear projection televisions. Combining these “microelectromechanical systems” (MEMS) with enzymes or other biologically active molecules produces sensors that can detect a wide variety of chemicals. Researchers at Clemson University are working on nanotech sensors that will glow in the presence of common food contaminants such as *E. coli* and *Salmonella*. Other nanotech sensors have been made to detect glucose, screen RNA, and scan for cancer biomarkers in the blood. A group at the University of Rochester is developing nanotech biosensors to detect biowarfare agents such as anthrax and release counteracting drugs.

There is a darker side to nanotechnology as well. In theory, nanotech could be used to build artificial pathogens. Inhaled, nanotech “viruses” would bore into the lung tissue, either destroying the capacity to breathe or traveling through the blood to commit cell-sized mayhem at distant locations. With enough information about the target, nanotech weapons could be designed to “take out” a single individual in a city of millions, even though the victim’s exact location remained unknown. Other nanomechanisms could be used to position explosive dust so as to provide the biggest possible impact from a dust/air bomb. This smart, malignant dust could even infiltrate underground bunkers and other well sealed targets. Still more destructively, nanotech could be designed to “eat” concrete, steel, or lubricants. An adversary’s economy would soon grind, literally, to a halt, if his buildings and bridges did not simply collapse around him. These threats are unlikely to materialize within the next five years. Yet tomorrow’s police forces will have to head off these attacks as well as simple bombings, and its other first responders could have to deal with them.

For police and intelligence work, sensors are the core of nanotechnology. In five years, they will still be largely experimental. However, in ten years nanoengineers will pack mass produced sensors, a power supply, and a communications channel to report the sensors’ findings into a volume of 1 cubic millimeter or less. Some will simply listen to their surroundings, transmitting conversations to nanotech relays, and eventually to a

recording station. Others will “sniff” for traces of explosives or flammable materials.

A decade further out, it may be possible for nanotech sensors to recognize DNA or other bio-indicators and report the presence of a single individual of interest if he appeared anywhere within their range. Others will be hyperspectral, multisensor swarms that make it impossible to enter a restricted area without detection. In 20 years, such devices will be cheap enough and versatile enough to deploy en masse wherever someone needs to collect information. We will have entered an age of ubiquitous sensors, providing essentially global coverage to anyone who can afford the very modest tab.

Trends in RFID

Unlike the other technologies considered here, RFID--for "Radio Frequency Identification"--tags are about as prosaic as high-tech can be. Part computer chip, part radio transmitter, an RFID tag can store information and respond to queries from an RFID transceiver. When you speed through a highway toll or pay for gas with the wave of a key fob, an RFID chip has told the toll or gas-station system whose bank account to tap for payment. Wal-Mart, Best Buy, and other mass marketers are forcing their suppliers to use it, thus streamlining their own inventory and order systems. MasterCard, Visa, and American Express are using it in “smart” credit cards. The U.S. government wants it built into the world’s passports. And many industry observers believe that it will trigger a revolution throughout agriculture, manufacturing, and services alike.

Think of RFID as a sort of super-barcode that can be read at a distance, even when it is hidden from the reader’s line of sight. RFID tags can store, and report, almost any information that could interest a user. Mostly, they just identify the item they are attached to, so shippers can track their location, much as UPS and FedEx use bar codes. Yet far more is possible. Embed an RFID tag in a car key, as Toyota does with the Prius, and you can program the car not to start unless the proper key is in the ignition. Embed it in a police officer's gun, and no criminal will ever be able to use that weapon. Tag your workers, and RFID-coded locks can keep unauthorized personnel out of sensitive areas. Tag passports or credit cards, and you make fraud and illegal border crossing a lot harder. Tag cargo containers after inspection in foreign ports, and you can be sure no one has opened them later to smuggle a bomb into the United States or another target country. Add the appropriate sensors, and an airplane flying over the cargo ship can detect whether a container now holds explosives or has been exposed to a source of radioactivity.

The most advanced RFID tags are scarcely bigger than a grain of sand. Soon they will not be much more expensive. Eventually, everything on the planet could have its own unique RFID identifier feeding into a database of information about where it has been, what conditions it has encountered, and even who has handled it, or even been nearby.

The applications for law enforcement and intelligence work are obvious. Cheap, tiny RFID chips, some of them coupled to wireless digital sensors, can monitor anything

or anyone deemed important enough to bother watching. Commercial use of RFID chips already is an issue of concern among civil libertarians. Use by police agencies will be an even greater worry. But it also will be an extremely useful tool for the prevention of terrorism, and the source of an overwhelming flood of data to be stored, catalogued, searched, analyzed, and eventually perhaps taken to court.

Trends in Biotech

Beyond DNA testing, biotechnology has few direct applications to police work. Yet it will wreak enormous changes in the world that law enforcement tries to monitor and control. By far the greatest concern is likely to be the potential for the development of biotech weapons. Bacteria, viruses, prions, parasites, fungi, and other pathogens and biological toxins could easily be genetically engineered for increased virulence and drug resistance. Even binary bioweapons are under study. Like binary nerve gasses, they are safe until the two primary ingredients are mixed; then they become deadly. Another chilling possibility would be the creation of genomically targeted pathogens, designed to wipe out a specific population with little or no effect on others. Hitler would have loved the concept. So would some of today's more pathological villains.

Bioweapons have at least two advantages that many other high-impact weapons do not. One is their relative ease of development. Although it takes enormous skill to tailor and weaponize a pathogen, the necessary equipment and materials are well within reach of even a modest corporation. Several years ago, one company even marketed a genetic engineering kit for high school biology classes. There is no reason individual biologists could not develop their own DIY biological warfare program.

The other advantage is anonymity. Once a biological agent has been released, it is very difficult to track back to its source. This would be particularly true of a bioweapon from a clandestine development program, but that level of secrecy is not really necessary. Even knowing that the anthrax strain used in the 2001 incidents was created in a government-operated laboratory, American authorities still have not been able to track down the culprit who mailed anthrax-laden letters to journalists and politicians. Preventing more such attacks in the future will require good intelligence work to identify any possible bioterrorist before his plan can be carried out.

Trends in Energetics

Non-nuclear explosives for mass effect will appear in the near future. These include:

- Fuel-air and dust-air bombs with explosive power 15 times as great as the same weight of TNT. The first such devices already are available.
- Metastable interstitial composite (MIC/cubanes), with about six times the power of TNT.
- Strain-bond energy release explosives, with around 100 times the power of TNT.

- And perhaps a metastable isomer called hafnium-178. In theory, a kilogram of Ha_{178} could deliver as much energy as 250 tons of TNT. Unlike conventional explosives, all of this energy would be released as hard gamma rays, effectively sterilizing the surrounding area without harming useful structures. There is some debate over whether this theoretical possibility can ever be realized.

Even if the horror of hafnium-178 never materializes, tomorrow's unconventional explosives will bring a new level of destruction to forms of attack that already are potent enough. Early in the Iraq War, a platoon of American infantry using a bazooka-like weapon firing missiles tipped with fuel-air warheads reported bringing down a sizable single-story masonry building with just one hand-carried rocket. Now imagine the effect of a fuel-air car bomb. In five years, we might not have to imagine such an attack. We may be able to watch its results on the evening news.

Trends in Information Technology

Of the four technological revolutions considered here, the growing capability of computers and computer networks will have by far the greatest impact on police and security functions. We have been feeling that revolution for more than a decade. It can only accelerate in the years ahead.

Consider first the raw power of computers. It took 42 years, from 1959 to 2001, for computer speed to increase by a factor of 1 million. According to Dennis Bushnell, chief scientist at NASA's Langley Research Center, computing power is likely to grow by a factor of 100 million by 2030. Cray promises to market the first computer capable of sustaining petaflop computing speed— 10^{15} calculations per second—by 2010. In Mr. Bushnell's timeline, by 2010 computers will be capable of 20 petaflops, 20 thousand trillion calculations per second. This is roughly equal to the computing power of the human brain. Fifteen years later, that power will be found in a personal computer. By 2030, he says, the personal computer will have computing power equal to a town full of human minds.

The development of vastly more powerful computers is an important way in which information technology will change in the coming years, but it is only one of many. Others also will have implications for information-based police work.

One is further progress in data compression. Given the size of today's archives and the growth in data collection expected for the near future, more efficient compression techniques that minimize loss of resolution, particularly in images, may be the second most important development in computing to be expected in the years ahead. Today, this is mainly a challenge for organizations such as the National Security Agency, which processes and stores images collected by American spy satellites. In the

future, and probably the near future, it will be a problem for the police departments of major cities that collect images from networks of surveillance cameras and will be expected to keep them for analysis and potential use as evidence in court.

Another new demand for storage and processing power may come from DNA testing. According to recent studies, 41 percent of felons have at least one close relative who also is a felon. Among some minorities, the number rises to 50 percent. This raises the possibility of identifying criminals from DNA evidence even when their own samples are not on file, by scanning through the genetic records for samples from their relatives. The FBI will not permit its agents to check familial DNA unless they have an exact match for the sample in hand. However, the Bureau will send samples to states, many of which allow scanning for familial DNA. Although the American Civil Liberties Union and other privacy advocates oppose familial DNA testing as an invasion of the privacy of innocent citizens, the practice seems little different from investigations based on partial matches of fingerprints or license plate numbers. We believe that many more jurisdictions, including the federal government, will adopt familial DNA searches in the next few years. As they do so, the demand for data storage and high-powered search software will expand yet again.

Although the capacity of long-term computer storage will continue to climb rapidly in the next 15 years even as its cost declines, the volume of data collected is likely to grow even faster. Without efficient compression, no one but the National Security Agency would have much hope of storing data long enough to figure out whether it is worth retaining.

However, data compression alone will not solve the problems of information glut. It must be coupled with advances in the ability to catalog, index, find, and retrieve all that stored information.

Already, analysts in the intelligence community are overwhelmed by the amount of raw data collected each day. Archives produced by surveillance satellites alone are in the petabyte (10^{15} bytes) range. Add in the products of open source intelligence, signals intelligence, measurement and signatures, human intelligence, and other sources, and the total is many times larger; we have seen no credible estimate of the total mass of data collected by the American intelligence services. Yet, even the most optimistic guess suggests that no less than half of that data is wasted because there are too few people to process it into useful form and pass the results along to those who need them. Some sources put the number at 80 percent.

Compared with this enormous burden, police forces have it relatively easy. Yet as the need to recognize and avert possible terrorist attacks grows, forces in large cities will find it increasingly necessary to gather data, correlate it with information obtained by other agencies, build a partial picture of whatever is really going on, and draw the appropriate inferences from it. Even law enforcement personnel in smaller communities will need to be familiar with these technologies, and have access to them, for the rare occasions when they are needed.

In the absence of a vastly larger workforce, this means developing automated systems to help in gathering and analyzing information. More than

one daunting task is involved here. The goal of easing law enforcement's access to and use of data requires solving many challenges, each composed of subtasks that may themselves require theoretical breakthroughs to accomplish.

In 2002, researchers Richard V. Badalamente and Frank L. Greitzer at Battelle Pacific Northwest Division conducted a workshop to identify the intelligence community's most pressing needs for new analytical tools. They identified ten high-priority needs that, in their view, would provide the greatest payoff. In the era of terrorism, many of these tools also could help law enforcement to make sense of their observations. The list includes:

Tools for seamless data access and conversion on the fly, to move from one database to another without having to log in to the new source or to use more than one query language in their research;

Diverse data ingestion and fusion systems that can treat text, photographs, maps, transcripts of telephone conversations, and many other forms of data as "information units" that can be combined into a single report and analyzed as a single mass of information;

Shared electronic folders for collaborative analysis by specialists in many different, often distant, facilities;

Tools that would coach users in the formulation and testing of possible explanations for the data they have uncovered and—ideally—alert them to any new information that may be relevant to the study;

Coaching tools to assist in developing a plan of attack for complex, long-term analyses;

Databases of the special skills and experience that colleagues in other agencies could bring to bear in making sense of possible terrorist events in the making;

Automatic updating, so that relevant new data can be added to the analyst's inquiry without repeating data searches;

Intelligent tutor software to help in analyzing data in a rigorous way that other authorities will be able to follow and understand;

Better ways to store, categorize, tag, organize, and process images obtained from diverse sources, such as satellites, lamppost surveillance cameras, and fingerprints;

An intelligence analysis knowledge base that can tell how other workers have already solved problems similar to the task at hand.

Today, only relatively primitive data access tools are available to local law enforcement. For example, the LInX "super database" soon will tie together a large number of databases maintained by regional agencies around the country. John Kapinos, of the Fairfax (VA) County Police Department, explains:

"It was discovered by after-the-fact records searches that some of the 9/11 terrorists had recently been stopped by state and local police officers for traffic violations. It was also true that some of these actors were known to Federal intelligence agencies, but in some cases had dropped off the radar. Imagine that

now, a patrol officer stops such an individual for a routine traffic violation and issues him a ticket. That ticket goes into the FCPD records system, with the violator's name, address, etc. That record then is 'pushed' out into a database tied to the LInX system, where it registers a hit with a name on a database maintained by the FBI. It turns out this guy was previously a subject of intelligence indicating that he had ties to a foreign terrorist group, but nobody knew he was in the U.S. Now we know he is, and where to start to look for him."

LInX is nearly active in the Washington, D.C., region, and it or similar systems should be available throughout the United States well within the next five years. This kind of unified data access will be extremely useful—not a revolution, but a solid incremental gain—in both antiterrorism and conventional police work.

Another incremental gain will come from computerized training methods. "Future training for all law enforcement agencies will be computer-based and will utilize scenarios and simulations," says the FBI's Alan Young. "The US military is already utilizing game simulators such as *Battlefield 2*. Simulations will become more realistic and involve terrorist and cyber crime threats. Decision-making will become more complex and involve multiple scenarios and threats." This practice in decision-making in real time and under something that resembles true emergency conditions should go a long way to improve the response to future terrorist events and natural disasters. Developing these training programs and distributing them to local law enforcement and security personnel will be one more task for the Department of Homeland Security.

Yet, as we have seen, far more is at least theoretically possible—and desperately needed. There is no way to be sure when any of these tools will become available, much less how quickly they will filter out from the rarefied heights of national intelligence to the blue-collar world of local law enforcement. Yet work on all these tasks is well under way. If the results do not appear within the next five years, they are almost certain to arrive within the working lives of today's younger officers.

That day will come none too soon. We are about to enter an era of ubiquitous sensors that can keep track of every human being on Earth, every vehicle, every package. Yet even that is far from being a formula for safety. The smallest countries will have the power, if they want it, to inflict crippling damage on the largest, while single terrorists or tiny cells, all but undetectable, will have access to explosives, bioengineered pathogens, and probably other weapons capable of inflicting casualties that formerly would have required an army.

These numerically tiny, but enormously powerful, threats—individuals and small cells—will be the greatest dangers that law enforcement must face in the years ahead. They also will be the greatest challenge it must cope with.

CONCLUSIONS

In the years ahead, international terrorism will continue to grow in many ways. The number of terrorists will grow as the Iraq War winds down and extremists trained in that hard and practical school return to their native lands and teach others their trade. The number of terrorist cells, each tiny and nearly impossible to detect, will grow as individual extremists develop ideas for attacks and recruit just one or two sympathizers to help with their plans. The number of incidents will grow as this new generation of terrorists spread out across the world to press their causes. And the challenge for law enforcement, even down to the local level, will grow at each step of the way.

The effective end of the Iraq War also will free something more useful than terrorists for other purposes: federal funding. Much of the \$100 billion or so being spent in Iraq each year will go to repair the national budget deficit. Much will go to fund the usual variety of subsidies and special interests that feeds at the federal trough, no matter which party is in power. Yet the obvious political need to prove that the next presidential administration is firmly against terrorism and on the side of national security will ensure that a bit of this surplus money goes to fund the law enforcement community. Some will be spent on communications equipment, some on providing new tools for data collection and analysis, some on hardening potential terrorist targets around the country. This should slightly ease the financial burden now being borne by state and local governments. And because it is politically useful to do so, much of this money is likely to be directed where it will do the most good, rather than according to the current policy of "everyone gets a piece of the pie." However, even with the costly Iraq War out of the way, the federal budget will never be so flush that all critical needs are adequately funded. States and local communities will continue to carry much of the cost of terrorism-related police work. Bridges, tunnels, subway systems, and even private facilities such as chemical plants will continue to be defended primarily by local law enforcement. The cost of doing so will come primarily from local budgets.

One of the most useful expenses may go for the acquisition of communications vans similar to the Mobile Emergency Operations Vehicles (MEOVs) now used by the Department of Homeland Security and stored at six locations around the country. MEOVs are mobile, self-contained communications systems that can link emergency managers to first responder units, even when those units are equipped with incompatible radio equipment. Most major cities now are equipped with these or similar units, but there is no guarantee that future terrorist incidents or other emergencies will conveniently occur in one of these locations. At Forecasting International, we believe that each state needs at least two of these vehicles on hand to coordinate emergency response teams in time of need. These vehicles could be stored with National Guard units to be dispatched when and where they are required.

However, for day to day policing and interception of potential terrorist events, the highest priority clearly is to link local law enforcement agencies with national resources, and to provide training in their efficient use. Every police force should be tied into one of

the regional Fusion Centers such as the National Capitol Regional Intelligence Center. Major forces from large cities need to delegate one or two officers permanently to this task. Smaller communities may find it necessary to settle for assigning a single officer to cultivate contacts with the nearest Fusion Center as a part-time resource that can be tapped as needed.

Of the nearly \$797 million distributed by Homeland Security's Urban Areas Security Initiative Program in FY2007, 55 percent—nearly \$411 million—goes to just six major cities and their surroundings: the San Francisco Bay area, Chicago, Houston, Los Angeles/Long Beach, Washington, D.C., and New York City/northern New Jersey. These regions offer many obvious targets for terrorists, and they extraordinarily complicated security structures, with responsibilities shared by many local agencies that may not be accustomed to cooperating effectively. As a result, these major cities hold frequent training exercises for their first responders. These often are coordinated with state and federal authorities, the Department of Homeland Security, and other emergency response agencies.

Similar communities can rarely afford the time or money to duplicate these efforts, even on their own scale. Instead, they can delegate representatives to attend exercises held in the larger communities, learn how major emergency responses are coordinated, find out who to contact at the Department of Homeland Security and other federal agencies, and learn how best to use the resources available for disaster recovery. Designating one or two police officers and other officials to keep up with the "best practices" in emergency response and recovery, and to build contacts with state and federal response units, could go a long way to eliminate problems and promote efficiency if a terrorist attack or other disaster ever does strike the community.

Similarly, each law enforcement agency will need someone who is familiar with the new technologies becoming available for data collection and analysis, and who cultivates a high index of suspicion with regard to unusual activities that could be linked to terrorism. Five years from now such individuals may well be local law enforcement's most valuable weapon in the fight against terror.

BIBLIOGRAPHY

Cetron, M.J. and Probst, P.S. (1994) *Terror 2000: The Future Face of Terror*. Report of the 4th Annual Defense Worldwide Combating Terrorism Conference. Office of the Assistant Secretary of Defense, Special Operations and Low-Intensity Combat, Washington, D.C.

Cetron, M.J. (2005). "Holy Terror: Thinking the Unthinkable; Revisiting *Terror 2000*, the 1994 SO/LIC Report." Presented at the 15th Annual Defense Worldwide Combating Terrorism Conference.

Cetron, M.J. (2006). "Travel: Security, Safety, and Terrorism." Presented at World Trade Market 2006, London.

Cetron, M.J. and Davies, O. (2007). "The Worse-Case Scenario: An Alternative View." *The Futurist*. In press.

Davis, L.M., et al. (2004). "When Terrorism Hits Home: How Prepared Are State and Local Law Enforcement?" The Rand Corporation.

Davis, L.M., et al. (2006). "Combating Terrorism: How Prepared Are State and Local Response Organizations?" The Rand Corporation.

"D.C. Region Puts Homeland Security Grant to Work." WRC-TV. <http://www.msnbc.com/id/17859902/from/ET/>.

"Editorial: Sensible Security Fixes: What the Senate's latest homeland security bill does, and doesn't, include." (March 5, 2007) Washington Post, p. A14. <http://www.washingtonpost.com/wp-dyn/content/article/2007/03/04/AR2007030400973.html>.

Jensen, C.J. and Levin, B.H. (2007). "The World of 2020: Demographic shifts, cultural change, and social challenge." In J. A. Schafer (Ed.). *Policing 2020: Exploring the future of crime, communities, and policing*. Washington DC: Federal Bureau of Investigation, pp 31-70.

Levin, B.H. (2007). "Human capital in policing: What works, what doesn't work, what's promising?" In J. A. Schafer (Ed.). *Policing 2020: Exploring the future of crime, communities, and policing*. Washington DC: Federal Bureau of Investigation, pp 414-451.

Levin, B. and Jensen, C.J. III. (2006). "Homeland Security in 2015." In Buerger, M. E. (Ed.) *Homeland Security 2015: Proceedings of the Futures Working Group*, Volume 2. Washington D.C.: Federal Bureau of Investigation, pp. 9-25. [printed January 2007].

Report of the Official Account of the Bombings in London on 7th July 2005 (2006). London: The Stationery Office.

Riley, K.J., et al. (2005). "State and Local Intelligence in the War on Terrorism." The Rand Corporation.

Schafer, J.A. (Ed.). *Policing 2020: Exploring the future of crime, communities, and policing*. Washington DC: Federal Bureau of Investigation.

Tafoya, W.L. "The Coming Knowledge Revolution: Will Police Planners be Active Participants or Sideline Observers?" (2006). Presented at IALEP Conference 2006.

APPENDIX A: IDENTIFYING FUTURE TERRORIST RISKS

**Presented by Dr. Marvin J. Cetron,
President, Forecasting International
To the SAS Regiment at Swanbourne, Western Australia
May 10, 2005**

EXECUTIVE SUMMARY

In the last few months, two significant reports have looked at the kinds of attack that terrorists might carry out in the future. One was conducted by Forecasting International (FI), the other by the U.S. Department of Homeland Security (DHS). These efforts were designed to identify which possible terrorist attacks are most likely to occur and which would have the greatest impact on the target country. This information should assist the allocation of antiterrorism resources where they will have the greatest benefit. It also may reveal previously unrecognized opportunities to defend the country and its facilities abroad against terrorist events.

Although these studies focused on the United States, we believe they offer valuable insights for the future of terrorism in Australia, or in any industrialized country. Specific targets may differ—a hotel in Melbourne rather than one in Orlando, or a natural gas pipeline in Sydney instead of a pipeline in Houston—but the kinds of target that terrorists will prefer are likely to be similar from one country to the next. So is the chosen method of attack for each. This kind of information is vital for planning. Prior to this research, it had been hard to come by.

Critical events identified by the DHS study included blowing up a chlorine tank at an urban sewage treatment plant; spreading pneumonic plague in the bathrooms of an airport, sports arena, or train station; and infecting cattle with pneumonic plague.

FI's work found that the most likely attack was simply to create public unease by spreading rumors of an impending terrorist attack. However, more serious events came close behind. These included attacking Saudi oil production; coordinated suicide bombings in Washington, D.C.; general Internet overload; attacking commuter trains into New York or another major city; bombing one or more oil pipelines; and destroying the rail and auto tunnels that serve New York City. However, events with the greatest impact included:

- Setting off a suitcase nuclear bomb at any target;
- Shooting down Air Force 1;
- Setting off a "dirty bomb" packed with stolen radiological medical waste in a populated area;
- Detonating a liquefied natural gas tanker in Boston Harbor;
- And introducing nerve gas into the air conditioning of a major public building or office tower.

Each of these events was rated more likely to have a greater impact than the 9/11 attacks.

WORKING METHODS

The two projects differed significantly in their goals and in their approach to the work. The DHS sought to identify a limited number of events against which federal and state authorities should direct their resources because of their probability or their human and economic cost. That work was carried out by a cadre of DHS personnel with relatively little input from outside.

FI took a broader look at nearly 50 possible attacks and then surveyed several diverse groups of experts for their view on those events. We also asked them to suggest plausible attacks that we had overlooked. We did not attempt to provide specific body counts or dollar costs for the attacks, as the DHS team did, but instead sought to identify an expert consensus about which events were most likely or would have the greatest impact on the United States.

Our study combined some groups of experts whose views of the future are seldom compared. In the first stage of research, two major polls gathered data on the probability and impact of possible terrorist attacks. One surveyed participants at the annual meeting of the World Future Society, in July; it collected the views of nearly 100 leading forecasters. The second was carried out at the 15th annual Defense Worldwide Combating Terrorism Conference, held in September by the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict; it produced replies from 216 experts on counterterrorism, many of them extremely detailed. In later surveys, we also obtained responses from approximately 50 retired military officers, many of flag rank, and a number of executives in the hospitality industry, which has often been targeted by terrorists in foreign lands. The questionnaires for this study took into account both current efforts to secure the United States against attack and a variety of trends now changing the aims and capabilities of the international terrorist community.

In the second stage, FI analyzed the results of these surveys to identify the most likely and devastating assaults that America must be prepared to face. For each possible event, we examined the likelihood of an attack by four specific antagonists: a Native American organization such as Aryan Nation; a small, semi-independent terrorist cell linked to Al Qaeda; a major terrorist organization with global reach, such as Al Qaeda itself; and a terrorist group with state sponsorship.

The combination of forecasters and subject specialists is one that FI has often used with great success. In previous studies of terrorism, forecasters have been able to suggest many possible developments that might not have occurred to subject specialists, while terrorism experts have kept the research firmly rooted in reality.

For example, our ground-breaking *Terror 2000: The Future Face of Terror* was carried out in 1994 for the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. It predicted virtually the entire course of international terrorism as it has developed over the last ten years. Specific forecasts

included the rise of Muslim fundamentalism; a second, much more successful, assault on the World Trade Center; the use of multiple coordinated attacks aimed at causing mass casualties; and the deliberate crash of an airplane into the Pentagon. (That last item was removed from the final report at the request of the State Department.) Many of these insights were refined by terrorism experts from the suggestions of generalist forecasters. Many lay outside the consensus view of terrorism at the time and would have been unlikely to originate within the specialist community

RESULTS

The study by the Department of Homeland Security identified twelve possible terrorist attacks that its researchers felt required special attention from security personnel, either because they were particularly likely or because they would be especially devastating. Among the most serious:

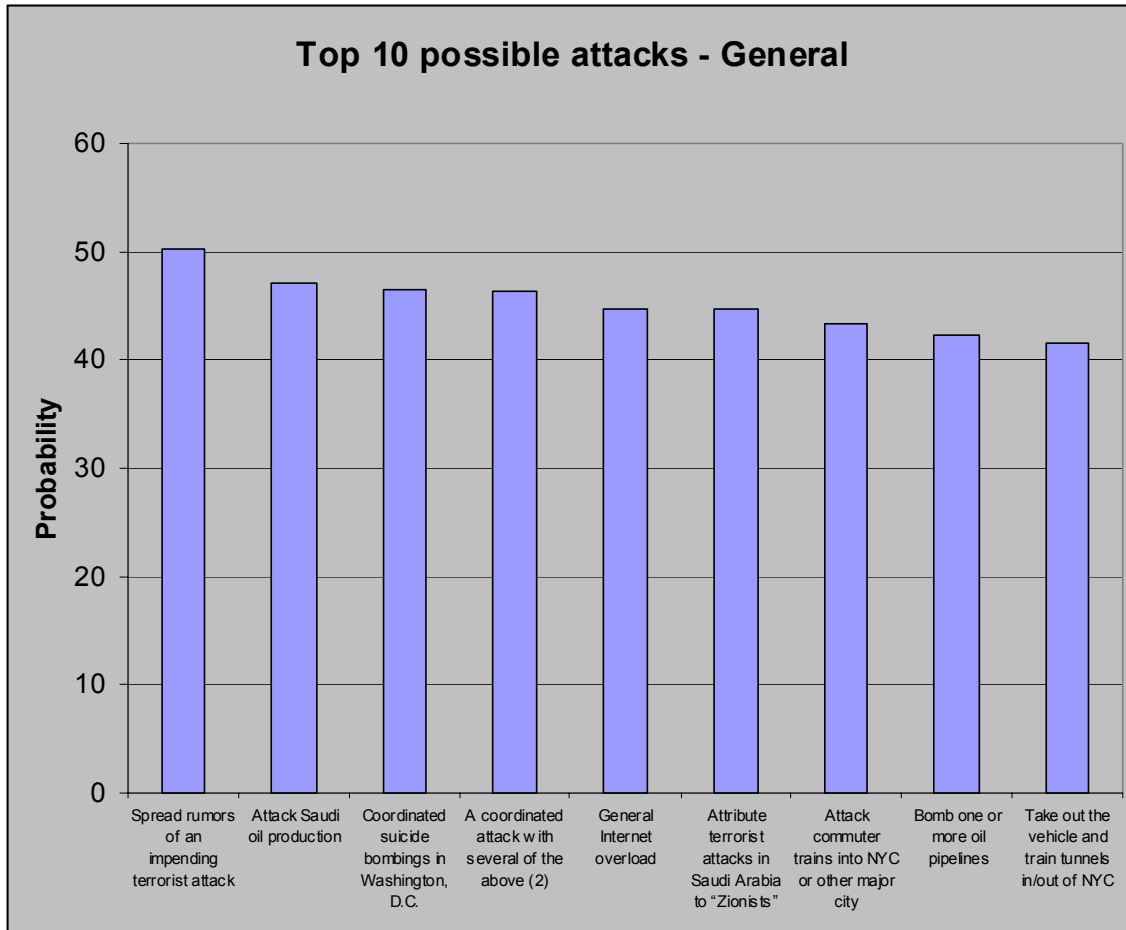
- Detonating a nuclear bomb, of course, was assessed as likely to be the most destructive attack, both in lives lost and in economic impact.
- Blowing up a chlorine tank at a big-city sewage treatment plant would release a cloud of toxic gas that could kill 17,500 people and sicken more than 100,000.
- Spreading pneumonic plague in the bathrooms of airports, sports arenas, and train stations would kill or sicken relatively few people—2,500 and 8,000, respectively—but its effects would be felt world-wide.
- Infecting cattle with hoof-and-mouth disease at several locations would cause hundreds of millions of dollars in losses.
- Spraying anthrax from a truck driving through five cities over two weeks would expose as many as 350,000 people to the disease. An estimated 13,200 could die.
- Detonating a “dirty bomb” packed with radiological medical waste would kill 540 people initially, but radioactive contamination would quickly spread over an area of 36 blocks, contaminating businesses and homes, schools and shopping areas, mass transit, and the urban infrastructure.

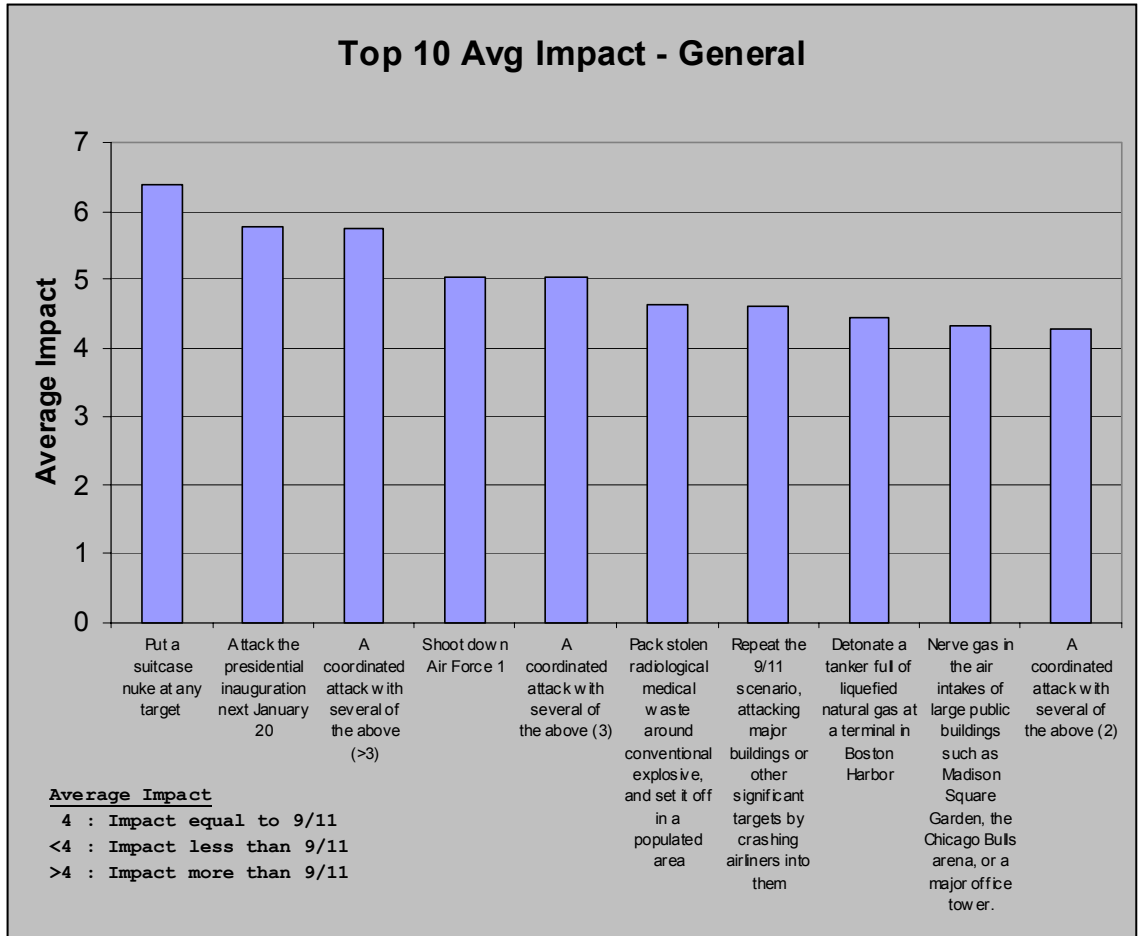
The study deliberately omitted some plausible attacks. For example, it did not consider an airline hijacking because plans for dealing with such an event have already been well refined. The goal was to identify unrecognized risks and figure out what how to deal with them. For each event, the study attempted to establish what kind of demands would be placed on the emergency response and public health systems. One section of the report listed no fewer than 1,500 specific tasks that might have to be performed in response to an attack.

Forecasting International’s study was more comprehensive than the DHS research in some ways, less so in others. It focused on the events themselves, and examined more than four times as many possible attacks. However, it left the demands

that would be placed on medical and emergency services for later examination.

The consensus results of our study are presented in the two graphs below. Their significance to Australia, and some related topics, will be considered in the summary that follows.





SUMMARY

As we can see in the graphs above, in Appendix A, and in results of the DHS study, there is no shortage of ways in which a terrorist group can spread death and destruction in a developed country. Many of them, such as the production of nerve gas, require a significant investment in technology. Others are within reach of a relatively small and unsophisticated cell. The bombing of commuter trains in Madrid was carried out by a small, independent group of extremists based in Morocco. It could be repeated in any city in the world by anyone capable of stealing dynamite from a construction site. Canberra, Melbourne, Sydney, and Perth all have extensive systems of commuter trains that would be difficult to defend against random bombing. Given the success of the Madrid bombings, we would rate a similar bombing as being perhaps the single terrorist event most likely to strike any major city.

Most of the other attacks considered in both these studies are as applicable to

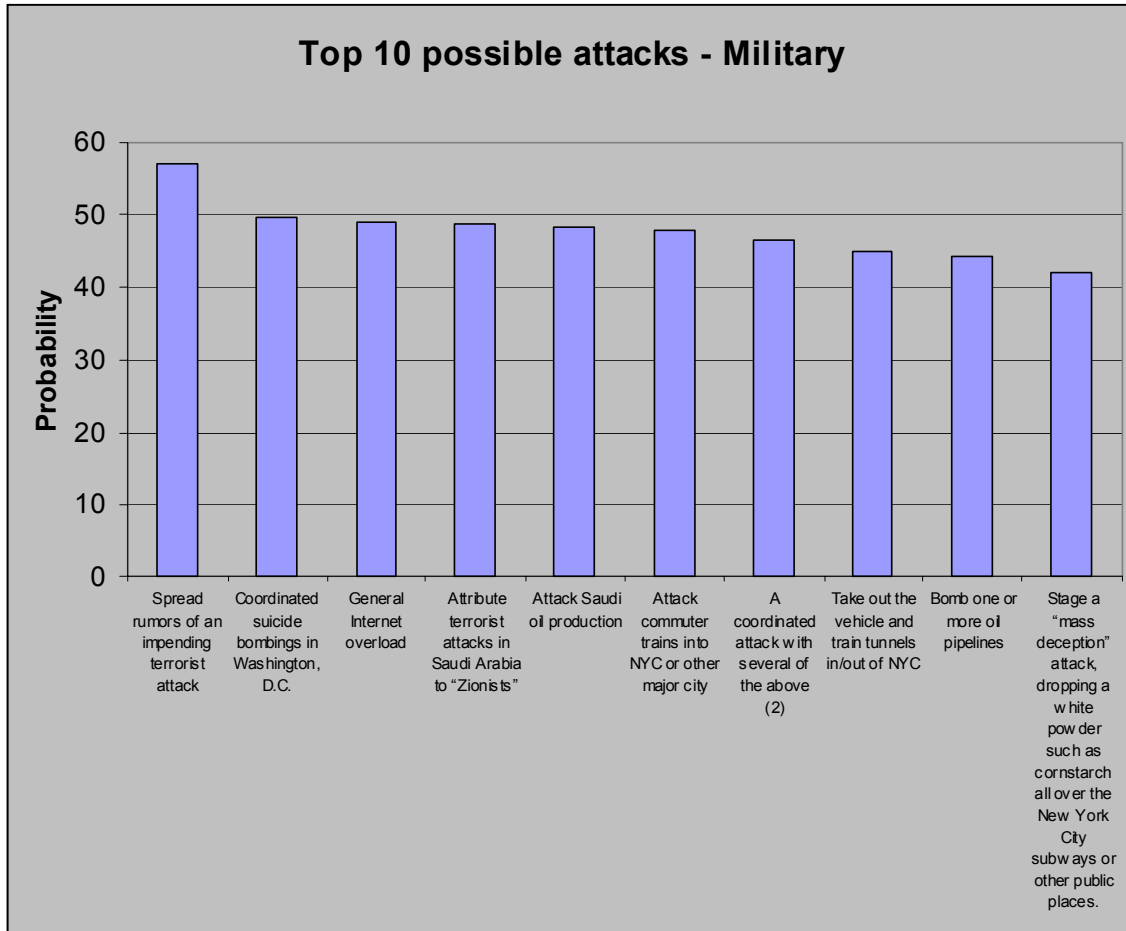
Australia as they are to the United States. Foot-and-mouth disease is as deadly to Australian cattle as it is to American cattle, and could be equally destructive to Australia's extensive sheep ranches. Radiological medical waste probably is no harder to steal in one country than in the other. Pipelines are easy targets in both countries; at least four run through Sydney, two that carry natural gas, one containing ethane, and one for oil. These potential terrorist targets all merit attention from Australian security personnel.

Given the rapid growth of Australia's Muslim population, two more points need to be made, though they have nothing to do with the studies above. Whatever terrorist attacks Australia faces in the future almost certainly will come out of the Muslim community. They may be committed by Muslim immigrants; they could originate with native Australian converts to Islam. Any heavy-handed attempt at surveillance or control makes such an event more likely, not less so. The United States made this mistake in the early days after the September 11 attack and has spent the years since trying to repair the damage. Muslims are not only the most likely source of trouble; they are the people most likely to learn of it before it occurs, and therefore are the most likely to be able to help in heading it off. They should be presumed to be loyal Australians, with the same rights that others enjoy, and cultivated as possible allies in the war against terror.

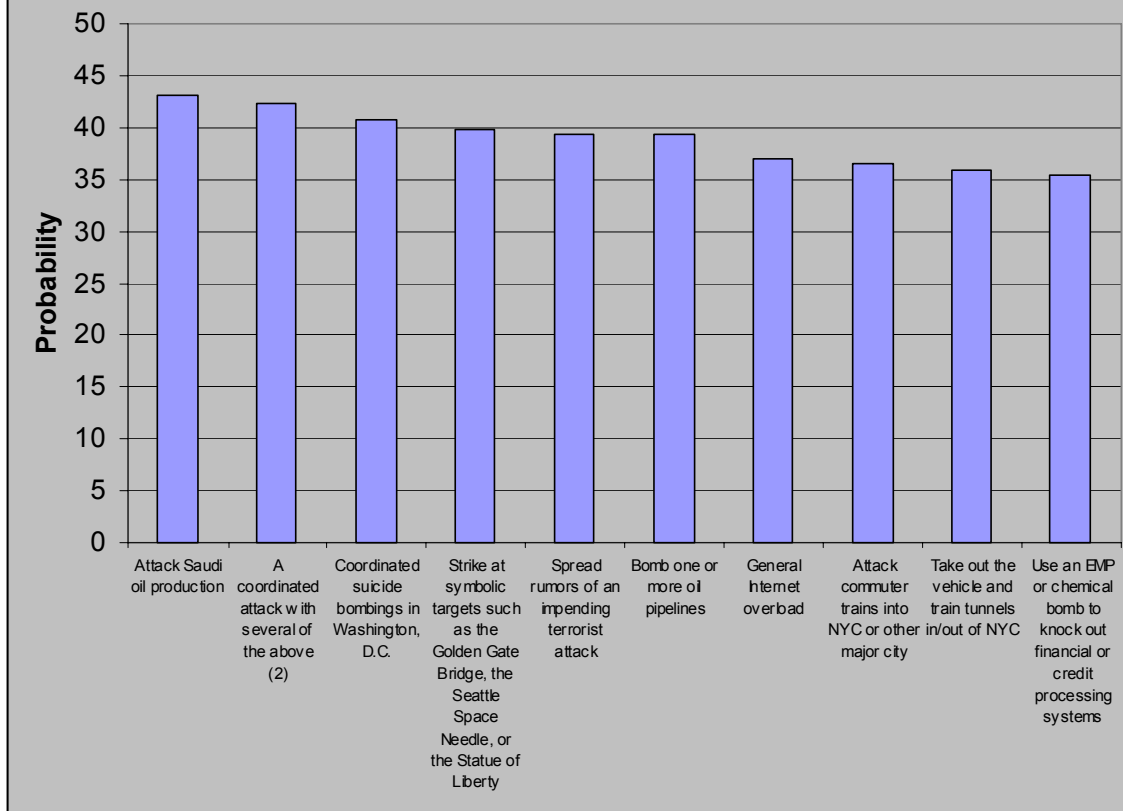
However, one group of people, Muslim or not, does require special attention. These are Australian Army personnel themselves, and particularly those charged with antiterrorism duties. No one has a better chance to do harm than those who are trusted to prevent it.

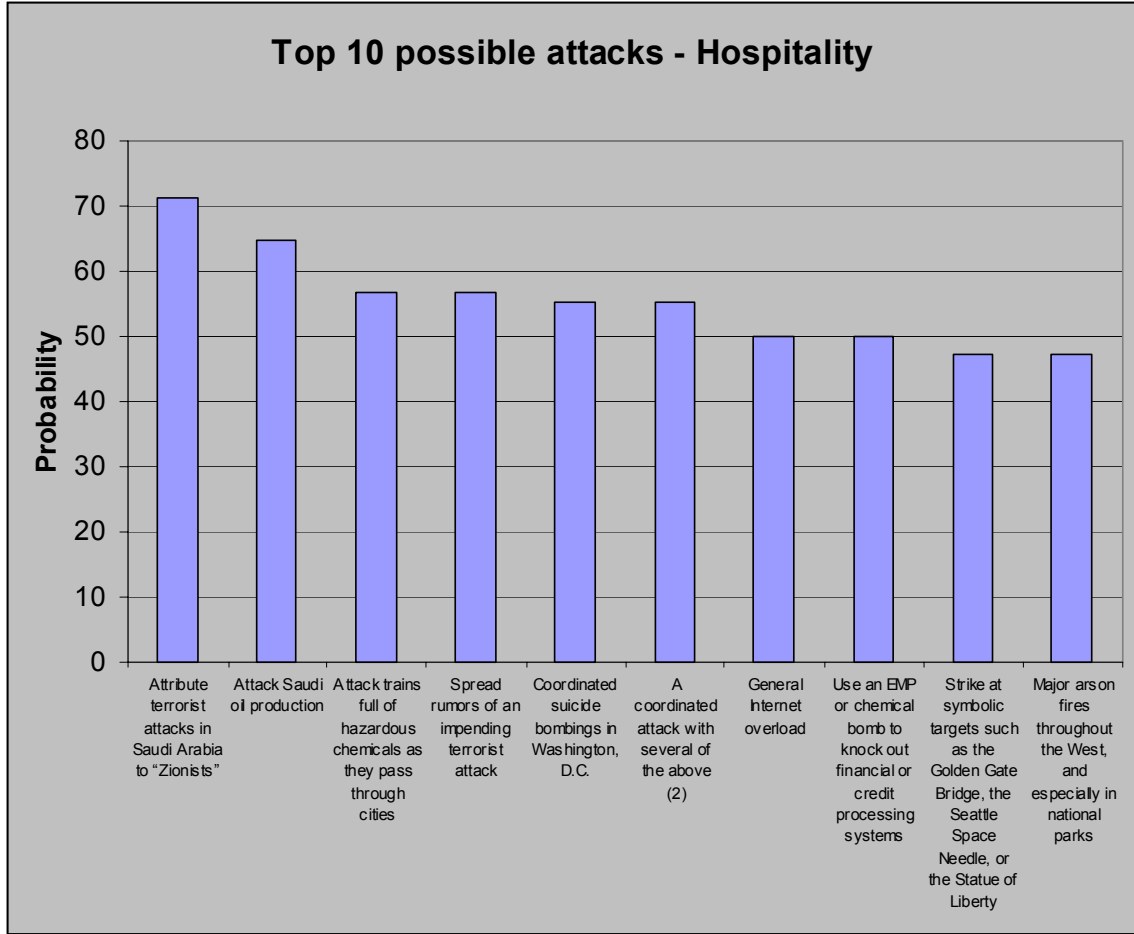
In the United States, we have seen the power that military personnel have to strike at our counterterrorist forces. In March 2003, Sgt. Hasan Akbar, then with the 101st Airborne Division in Kuwait, attacked his fellow troops with grenade and rifle. An Army captain and an Air Force major died in the attack, and 14 soldiers were wounded. Better security screening might have identified Sgt. Akbar as a potential problem long before he had the chance to act. Australian forces can learn from our mistake.

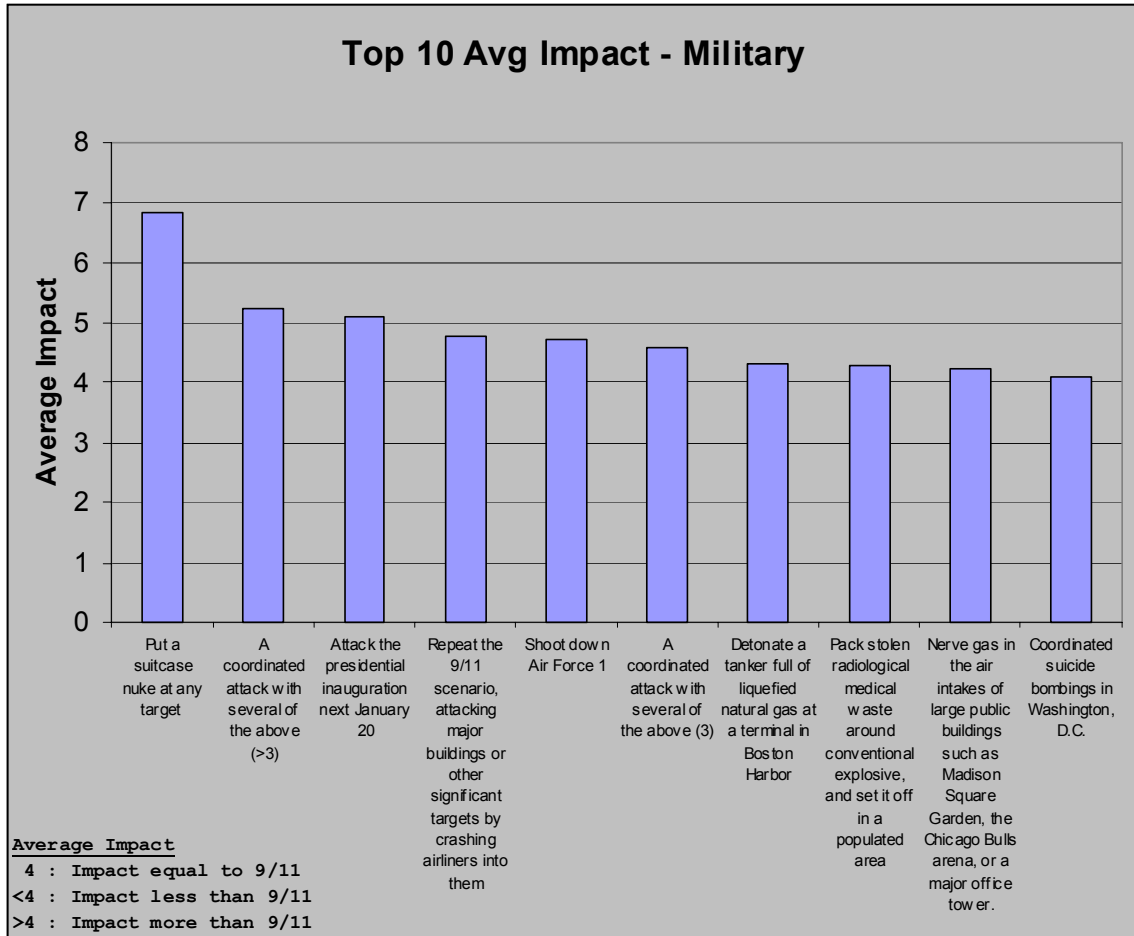
APPENDIX A: DETAILED RESULTS OF THE FI STUDY



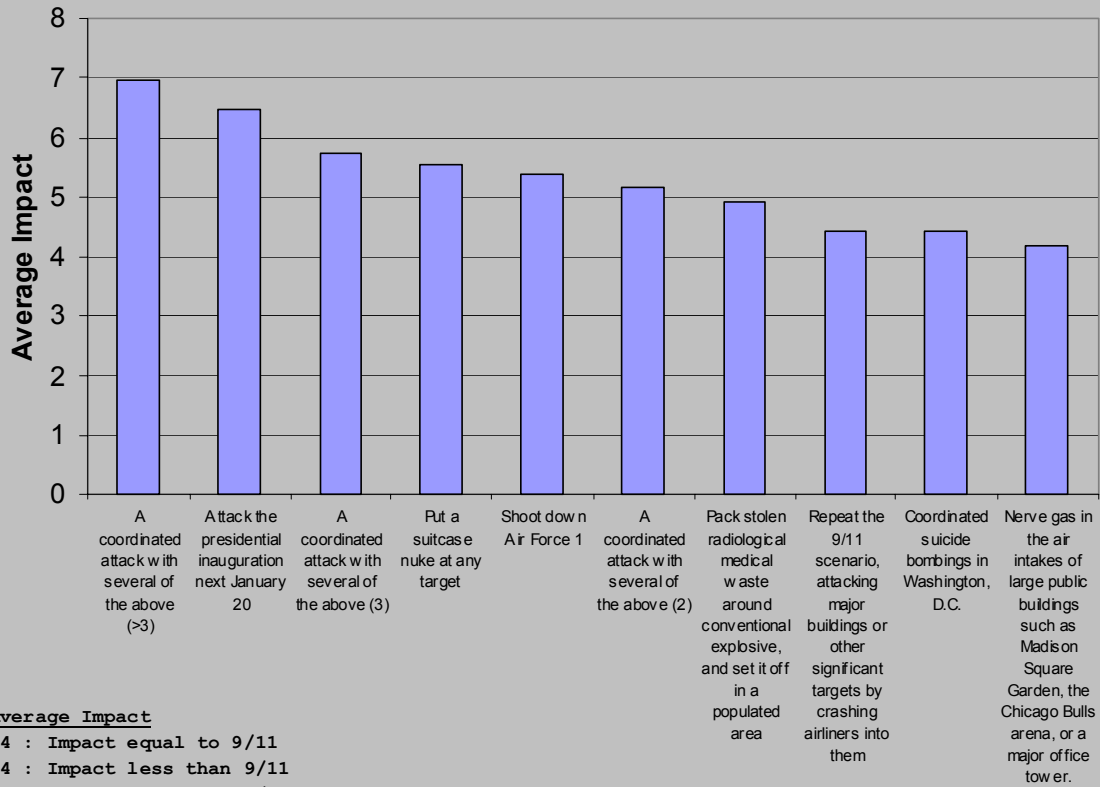
Top 10 possible attacks - Futuristic



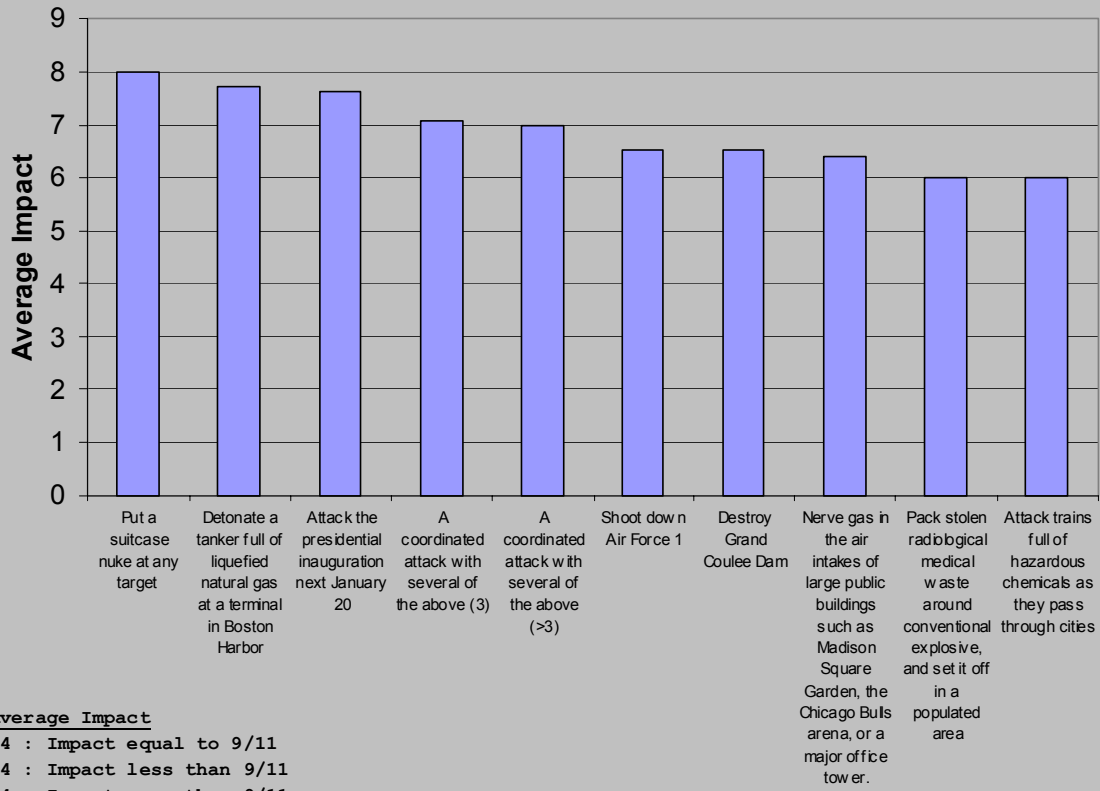




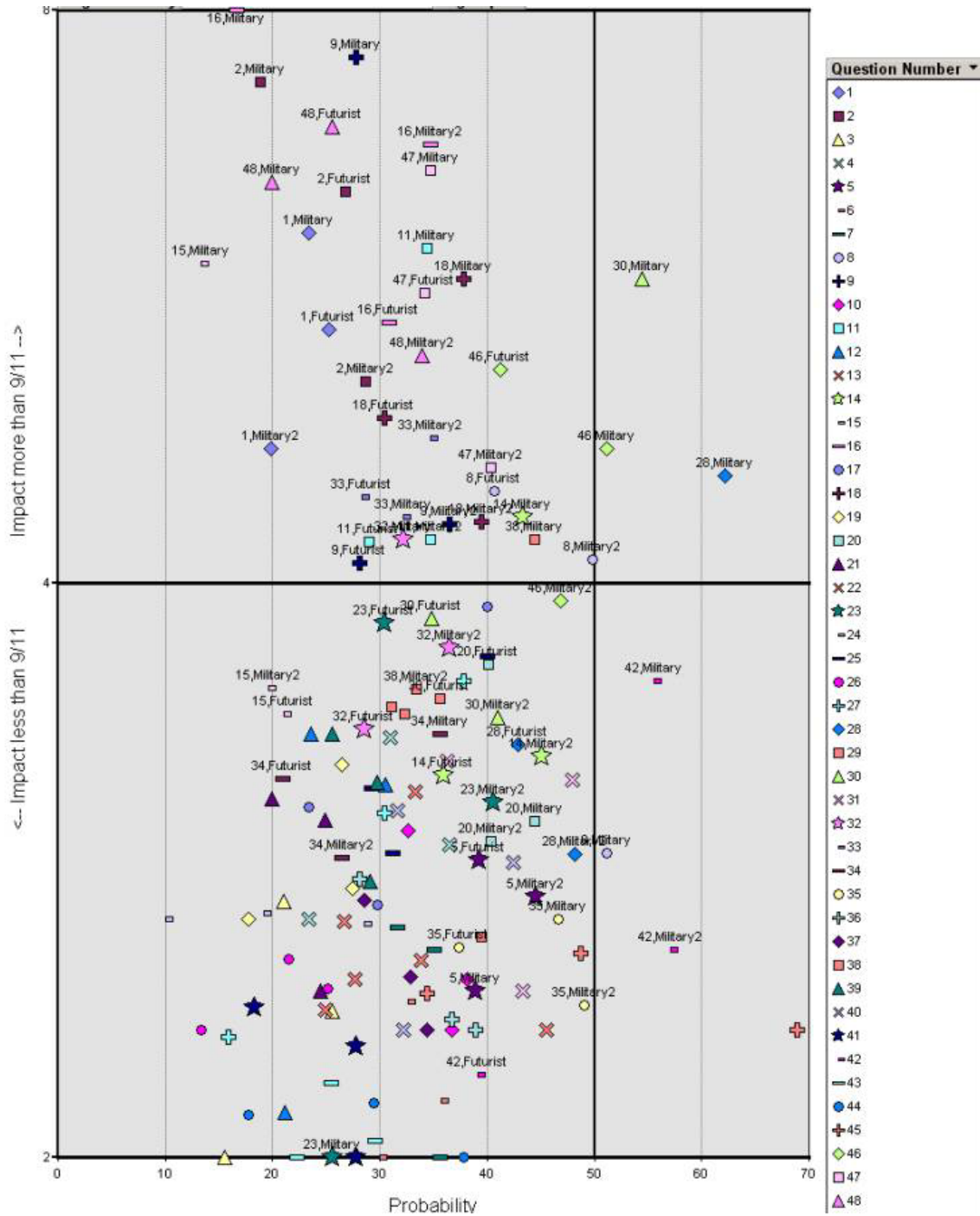
Top 10 Avg Impact - Futuristic



Top 10 Avg Impact - Hospitality



RAW DATA



POSSIBLE TERRORIST EVENTS

- 1 Shoot down Air Force 1
- 2 Attack the presidential inauguration next January 20
- 3 Take out the St. Louis Arch
- 4 Launch coordinated attacks on chlorine tanks at sewage treatment plants
- 5 Bomb one or more oil pipelines
- 6 Bring down one or more of the high tension wires across the Far West
- 7 Truck bombs at truck stops
- 8 Coordinated suicide bombings in Washington, D.C.
- 9 Detonate a tanker full of liquefied natural gas at a terminal in Boston Harbor
- 10 Simple tanker truck "accidents" on bridges across the Mississippi, Hudson, or other major rivers
- 11 Nerve gas in the air intakes of large public buildings such as Madison Square Garden, the Chicago Bulls arena, or a major office tower.
- 12 Mix blight or other plant disease into crop dusting
- 13 Chemical poisoning of metropolitan sewage plants
- 14 Take out the vehicle and train tunnels in/out of NYC
- 15 Destroy Grand Coulee Dam
- 16 Put a suitcase nuke at any target
- 17 Use stolen medical waste to contaminate reservoirs, swimming areas, or building air vents
- 18 Pack stolen radiological medical waste around conventional explosive, and set it off in a populated area

- 19 Target the locks on the St. Lawrence Seaway
- 20 Strike at symbolic targets such as the Golden Gate Bridge, the Seattle Space Needle, or the Statue of Liberty
- 21 Poison the food at Greenbriar Conference Center
- 22 Major arson fires throughout the West, and especially in national parks
- 23 Coordinated shooting attacks in Disneyworld and Disneyland
- 24 Using mosquito abatement trucks to spread whatever—just taint the tanks and let the regular workers do the dirty work
- 25 Take out a major cruise ship entering or leaving the harbor in Miami or New York
- 26 Bomb a semiconductor plant
- 27 Attack winning U.S. Olympians during a celebration on their return from Greece
- 28 Attack Saudi oil production
- 29 Attack American refineries with bombs or RPGs
- 30 Attack trains full of hazardous chemicals as they pass through cities
- 31 Attack commuter trains into NYC or other major city
- 32 Bomb a chemical plant upwind of a major city
- 33 Repeat the 9/11 scenario, attacking major buildings or other significant targets by crashing airliners into them
- 34 Introduce *E. coli* into McDonald's hamburgers in occasions all across the United
- 35 General Internet overload
- 36 Contaminate foreign products coming into the U.S.
- 37 Contaminate American products abroad
- 38 Use an EMP or chemical bomb to knock out financial or credit processing systems

- 39 EMP bombs in the Internet-critical region of northern Virginia
- 40 Stage a “mass deception” attack, dropping a white powder such as cornstarch all over the New York City subways or other public places.
- 41 Steal several crop-dusting airplanes, and destroy them so that they cannot be found
- 42 Spread rumors of an impending terrorist attack
- 43 Steal the identity of a government official or other obstacle to the terrorist cause
- 44 Hijack FedEx trucks, repaint them, and dump them.
- 45 Attribute terrorist attacks in Saudi Arabia to “Zionists”
- 46 A coordinated attack with several of the above (2 incidents)
- 47 A coordinated attack with several of the above (3 incidents)
- 48 A coordinated attack with several of the above (>3 incidents)

Page left intentionally blank

Appendix B: Revolution, flash mobs, and brain chips. A grim vision of the future

Richard Norton-Taylor
The Guardian
Monday April 9, 2007
<http://www.guardian.co.uk/science/story/0,,2053020,00.html>

Information chips implanted in the brain. Electromagnetic pulse weapons. The middle classes becoming revolutionary, taking on the role of Marx's proletariat. The population of countries in the Middle East increasing by 132%, while Europe's drops as fertility falls. "Flash mobs"--groups rapidly mobilized by criminal gangs or terrorists groups.

This is the world in 30 years' time envisaged by a Ministry of Defense team responsible for painting a picture of the "future strategic context" likely to face Britain's armed forces. It includes an "analysis of the key risks and shocks". Rear Admiral Chris Parry, head of the MoD's Development, Concepts & Doctrine Centre which drew up the report, describes the assessments as "probability-based, rather than predictive".

The 90-page report comments on widely discussed issues such as the growing economic importance of India and China, the militarisation of space, and even what it calls "declining news quality" with the rise of "internet-enabled, citizen-journalists" and pressure to release stories "at the expense of facts". It includes other, some frightening, some reassuring, potential developments that are not so often discussed.

New weapons

An electromagnetic pulse will probably become operational by 2035 able to destroy all communications systems in a selected area or be used against a "world city" such as an international business service hub. The development of neutron weapons which destroy living organs but not buildings "might make a weapon of choice for extreme ethnic cleansing in an increasingly populated world". The use of unmanned weapons platforms would enable the "application of lethal force without human intervention, raising consequential legal and ethical issues". The "explicit use" of chemical, biological, radiological, and nuclear weapons and devices delivered by unmanned vehicles or missiles.

Based on the unclassified literature, Forecasting International believes that electromagnetic pulse weapons (EMP) will be available at least ten years earlier than this report suggests; some of the necessary technology is available now. The other weapons technologies also will be available by 2025, if they are not available today.

For police departments, electromagnetic pulse weapons are likely to be the greatest concern. These are weapons of mass disruption. If one goes off near a communications center, cars and foot patrols will be out of contact for the duration. When used near data storage systems, personnel and criminal records will disappear, at least until they can be restored from off-site archives. This future hazard justifies a major effort to protect critical information, with the help of both the National Science Foundation and the Defense Advanced Research Projects Agency.

Technology

By 2035, an implantable "information chip" could be wired directly to the brain. A growing pervasiveness of information communications technology will enable states, terrorists or criminals, to mobilize "flashmobs", challenging security forces to match this potential agility coupled with an ability to concentrate forces quickly in a small area.

Ultimately, the implantable information chip will be technologically and economically feasible. However, we have no idea when. Implanting a chip and connecting it to the brain will be possible, even practical, within a few years. Doing so usefully will require figuring out how to get information in and out of the brain, and theoretical breakthroughs of this kind do not arrive predictably. Under the circumstances, 2035 probably is as good an estimate as any. We would not be terribly surprised if the breakthrough came ten years earlier or or surprised at all if it came 25 years later.

Once this obstacle has been overcome, the information chip still may not be socially feasible. While we recognize no basic moral or ethical implications not already involved with other Net access, social conservatism could block its use in the United States--in which case only the criminals will have it.

Flashmobs, of course, happen now in benign forms. It seems only a matter of time before criminals and terrorists adapt this phenomenon to their own ends.

It is not clear what, if anything the information implant may imply for law enforcement. At first glance, it seems most likely to be useful for information-oriented white-collar crimes, such as data theft and embezzlement. Its possible applications for terrorism require study. Once the technology is developed, it will be worth figuring out whether there is any way to disable it for known criminals and suspected terrorists. Implant users also may wonder how being caught in the field of an EMP weapon might affect them.

The only obvious answer to flashmobs is to monitor them through human intelligence, so as to react as fast as possible when some particularly creative criminal or terrorist finds a use for them.

Marxism

"The middle classes could become a revolutionary class, taking the role envisaged for the proletariat by Marx," says the report. The thesis is based on a growing gap between

the middle classes and the super-rich on one hand and an urban under-class threatening social order: "The world's middle classes might unite, using access to knowledge, resources and skills to shape transnational processes in their own class interest". Marxism could also be revived, it says, because of global inequality. An increased trend towards moral relativism and pragmatic values will encourage people to seek the "sanctuary provided by more rigid belief systems, including religious orthodoxy and doctrinaire political ideologies, such as popularism and Marxism".

This seems almost vanishingly unlikely. In any society, middle classes characteristically work within the system to make certain that they benefit from it. It takes a lot to get the middle class motivated to overthrow the social order that supports them. That is the last change seen before a revolution, as it was in Iran before the fall of the Shah.

Based on studies by Forecasting International, a much more valuable indication of social instability is the gap between the incomes of the richest and poorest tenths of the society. The smaller that gap, the more stable the society will be. Once the average income of the upper tenth is more than 60 times that of the lower tenth, revolution becomes much more likely. The CIA World Factbook now uses this measure, pioneered by FI, to help gauge the stability of nations.

This is the clearest possible argument for community policing. There is no way to measure the forces for instability other than to have the confidence of the community, so that people will discuss their concerns. However, monitoring the income gap between the top and bottom tenths of society can help analysts to recognize when they should be particularly alert for possible trouble ahead.

Pressures leading to social unrest

By 2010 more than 50% of the world's population will be living in urban rather than rural environments, leading to social deprivation and "new instability risks", and the growth of shanty towns. By 2035, that figure will rise to 60%. Migration will increase. Globalization may lead to levels of international integration that effectively bring inter-state warfare to an end. But it may lead to "inter-communal conflict" - communities with shared interests transcending national boundaries and resorting to the use of violence.

Urbanization is one of the oldest trends we see at work in the world today. It is particularly strong in China and, to a lesser extent, India. It is a force for instability, as migrants lose their connections with the community, and therefore with social norms.

Monitoring urbanization, as it applies locally, will be crucial for law enforcement in the years ahead. As the American population grows and migrates, many suburbs are coming to resemble cities, while some rural areas are reaching the population density of yesterday's suburbs. As a result, suburban police departments will have to do many of the same things urban communities have done for years. They will build and operate

more strike forces, hire more police officers, and cultivate more communication with city departments. Rural communities in turn will have to learn to operate more as their colleagues in the suburbs used to do.

Population and Resources

The global population is likely to grow to 8.5bn in 2035, with less developed countries accounting for 98% of that. Some 87% of people under the age of 25 live in the developing world. Demographic trends, which will exacerbate economic and social tensions, have serious implications for the environment - including the provision of clean water and other resources - and for international relations. The population of sub-Saharan Africa will increase over the period by 81% and that of Middle Eastern countries by 132%.

These figures match our data well.

Continuing international migration will require police departments to keep track of local immigrants, especially from hostile countries. They will also need to monitor what goes on in countries where many local immigrants originated, to understand the forces that are influencing their residents. For example, residents from Muslim countries, no matter how decent and well intentioned, could be blackmailed to aid terrorists by threats to their relatives at home. It also will be necessary to keep track of money transfers to home countries. In this respect, our model for the future is Europe, and especially Britain, whose close relationship with Pakistan exposes it to a greater risk of terrorism. Merely collecting data will not be enough. This is one more mandate for community policing and human intelligence.

The Middle East

The massive population growth will mean the Middle East, and to a lesser extent North Africa, will remain highly unstable, says the report. It singles out Saudi Arabia, the most lucrative market for British arms, with unemployment levels of 20% and a "youth bulge" in a state whose population has risen from 7 million to 27 million since 1980. "The expectations of growing numbers of young people [in the whole region] many of whom will be confronted by the prospect of endemic unemployment ... are unlikely to be met," says the report.

This is a recipe for more terrorism in the region, more emigration to the West, and very possibly more terrorism in the West. Oil money could fund a healthy change in the Middle East, if governments there begin to provide an effective safety net for the poor. If they do not, and there is little evidence to suggest that they will, the future is likely to be even more violent than the present.

Law enforcement will have to watch the age group from 18 to 28, and especially violence-prone young men. Those with substantial immigrant populations will have to monitor what is happening in the Muslim lands, communications with local refugee populations, and other indicators of potential trouble. Local police departments also will need to join in an international police data-sharing network. As it develops, this network will become much larger and more complex than INTERPOL.

As a side issue, if Osama bin Laden survives and can make his way home to Saudi Arabia, it is entirely possible that he could become the head of government in Riyadh. This would expose the West to even greater levels of terrorism and would guarantee the loss of Saudi oil to the Western economies.

Islamic militancy

Resentment among young people in the face of unrepresentative regimes "will find outlets in political militancy, including radical political Islam whose concept of *Umma*, the global Islamic community, and resistance to capitalism may lie uneasily in an international system based on nation-states and global market forces", the report warns. The effects of such resentment will be expressed through the migration of youth populations and global communications, encouraging contacts between diaspora communities and their countries of origin.

Tension between the Islamic world and the west will remain, and may increasingly be targeted at China "who's new-found materialism, economic vibrancy, and institutionalized atheism, will be an anathema to orthodox Islam".

We agree with much of the above, but believe that the future course of Muslim militancy will depend substantially on whether the Shiites or Sunnis win their conflict in the next four or five years. Thus far, the Sunni community has proved more tractable than the Shiite, if only marginally so. The bottom line is that a Muslim Reformation is needed. It must come from within. The only influence the West can have on this process is to work with those Muslim organizations that seem most willing to live peacefully with their non-Muslim neighbors and to develop a religious and social order more compatible with the modern world.

There is relatively little chance that China will become a significant target for Muslim attack, despite its current, limited, problems with Islamists in the northwestern region bordering the "stans." Beijing is capable of much greater ruthlessness than the West. If terrorism becomes a major annoyance, it will simply eradicate the native population of the affected area to whatever extent it deems necessary and repopulate the region with ethnic Chinese, much as it has done in Tibet. There is a possibility that this "cleansing" will drive Islamists now living in China to emigrate to the Stans and other Muslim countries, and from there they could migrate to Europe, Canada, and the United States, to become terrorists in the West. However, we believe that this is relatively unlikely and that it would represent only a modest increment in the level of risk that the target nations will face.

Police will have to monitor all information that can be gleaned from local Muslim communities, including what goes on inside their mosques. However, this does not mean treating local Muslims as suspects or potential enemies. Law enforcement must work with them as it would with any other citizens. This is not only the right thing to do, it is the safest course. If the majority community shuts Muslims out, we will produce our own fifth column of terrorist sympathizers. Also, the Muslim community represents our only chance to find out about potential terrorist events before they occur. Most contacts with the Muslim community should be handled by local police departments, as one routine aspect of community policing.

Iran

Iran will steadily grow in economic and demographic strength and its energy reserves and geographic location will give it substantial strategic leverage. However, its government could be transformed. "From the middle of the period," says the report, "the country, especially its high proportion of younger people, will want to benefit from increased access to globalization and diversity, and it may be that Iran progressively, but unevenly, transforms...into a vibrant democracy."

FI agrees, but the process will take a long time. The current policy of isolating Iran is likely to prove self-defeating. The United States must work with them politically through the United Nations, bringing Russia, China, and India--countries respected and influential in Iran--into the process. Contacts with Iran must be guided to show Iranian youth that the peaceful use of nuclear power is rewarded, but not the development of weapons.

Our comments on Islamic militancy, above, apply here as well. Law enforcement can only monitor what is going on in Iran and in the local Muslim community, leaving foreign policy to other authority.

Terrorism

Casualties and the amount of damage inflicted by terrorism will stay low compared to other forms of coercion and conflict. But acts of extreme violence, supported by elements within Islamist states, with media exploitation to maximize the impact of the "theatre of violence" will persist. A "terrorist coalition", the report says, including a wide range of reactionary and revolutionary rejectionists such as ultra-nationalists, religious groupings and even extreme environmentalists, might conduct a global campaign of greater intensity".

This paragraph is half right. We will face more terrorism from Muslim extremists until we can get militant Islam under control. In the United States, we also will have problems

with PETA and the Aryan Nations, but environmentalists will be nothing like the Islamists. For a more detailed look at militant Islam, which will make it clear how this force differs from other extremist causes, see Cetron, M.J. (May-June 2007). "Defeating Terrorism: Is it Possible? Is it Probable?" The Futurist. Contact Forecasting International at marglo@tili.com for a copy of the article.

Again, the role of local law enforcement is to monitor their own Muslim communities and potential foreign influences on them, while making sure to treat them as ordinary Americans in all other ways.

Climate change

There is "compelling evidence" to indicate that climate change is occurring and that the atmosphere will continue to warm at an unprecedented rate throughout the 21st century. It could lead to a reduction in north Atlantic salinity by increasing the freshwater runoff from the Arctic. This could affect the natural circulation of the north Atlantic by diminishing the warming effect of ocean currents on Western Europe. "The drop in temperature might exceed that of the miniature ice age of the 17th and 18th centuries."

We concur, but the world is waking up to this issue. Carbon exchange programs may help to slow global warming or limit its effect, though this is by no means certain. The worst problems will be with water, especially in China.

This is an important issue globally, but it is of only secondary importance for law enforcement. It may act as a driver for future immigration, but will have no direct effect on communities. Local police should work with EPA to enforce environmental regulations, but even this is tangential to their basic activities.

End Note

This article, and the entire report to which it is appended, represents only a modest beginning of the examination of the future of law enforcement. Forecasting International believes that a much broader analysis is needed. As a start on this process, we can supply a list of 53 trends now changing the world. (E-mail marglo@tili.com for a copy.) It would be appropriate examine all of these trends for their potential impact on local police departments, and then to choose the ten or twelve most important trends and study their effects in greater detail.