TERRORISM AND ECONOMIC SECURITY

Robert Hutchings
Chairman, National Intelligence Council

International Security Management Association
Scottsdale, Arizona
14 January 2004

I would like to thank the President of the ISMA for the opportunity to address your association this morning. We live in turbulent and complex times. We possess unrivaled power, yet we remain vulnerable—as the terrorist attacks of 9/11 demonstrated so tragically.

The breakdown of the Cold War order thawed out historical problems that had been frozen over for decades. Globalization has brought with it enormous benefits, but it has also led to sharpened polarization between the haves and have-nots. Also, the very success of Western values has threatened in an existential way those who seek to preserve traditional ways of life in the face of modernity—ushering in **a new era of asymmetrical warfare** in which adversaries compensate for their relative military weakness by devising new strategies and adapting new technologies to exploit US vulnerabilities—the vulnerabilities of an open society.

These trends have imposed new challenges on the US Intelligence Community. And they have imposed new challenges on security professionals in American businesses to help keep US citizens abroad safe and our economy growing. Effective security management—on either the national or corporate levels—clearly hinges on our ability to identify, understand, and counter threats to our people, facilities, and interests. In some

cases, these threats are all too visible—as demonstrated by our recent experiences with elevated homeland security threat levels and "orange-alerts." In other cases, they are more subtle but no less ominous.

I would like to focus my remarks today on international terrorism, which I know is a preoccupation for all of you. I will begin with a "status report" in the war against terrorism, from the perspective of the US Government. Then I will offer some thoughts about the implications of terrorist dangers for American economic interests at home and abroad.

TERRORISM – A STATUS REPORT

First, a status report: we have made **great progress** in **the war against terrorism** since September 11. . . progress that has prevented the loss of many lives but that is causing dramatic changes in the nature of the challenges we face.

- We have **disrupted scores of plots** at home and abroad—plots that were audacious in terms of the numbers of attacks under consideration and their global scope.

- **Al-Qa'ida is in disarray.** More than two-thirds of its senior leaders, operatives, and facilitators are dead or in long-term custody. Those remaining are in hiding, their

ability to function constrained by physical isolation, disrupted communications, and reduced access to funds.

To put this in business terms, imagine that you are trying to lead a multinational enterprise. Almost all of your senior leadership is gone. You have no one you trust who can fill in. You cannot communicate with your subordinates. Your ability to conduct business is suffering and your shareholders are beginning to question whether their investments will ever pay dividends.

Despite this progress, the global war on terrorism will be a long fight and other organizations are increasingly adopting al-Qa'ida's ideology to attract new, young recruits. As we adapt our tactics, the terrorists are adapting theirs**.** They are trying to find new ways to share information and get funds. They understand that small ad hoc networks can still inflict significant damage.

Bin Ladin and many other al-Qa'ida terrorists see attacks that weaken our economy as key to undermining our strength and morale. In video statements after 9/11 we saw Bin Ladin marveling at the economic impact of the attacks, claiming New York lost over $1 trillion.

- Soft targets, including the US stock market, banks, major companies, and tall buildings are a primary focus of active al-Qa'ida planning. These softer targets are

seen as easier to hit than other high-priority targets, such as US Government buildings and major infrastructure targets, which have higher security postures.

- Targets such as nuclear power plants, water treatment facilities, and other public utilities are high on al-Qa'ida's targeting list as a way to sow panic and hurt our economy.

The group has continued to hone its use of transportation assets as weapons. We have found several examples of al-Qa'ida adjusting its tactics to circumvent enhanced airline security. Although we have disrupted several airline plots, we have not eliminated the threat to airplanes. There are still al-Qa'ida operatives who we believe have been deployed to hijack planes and fly them into key targets.

- Just this past year, al-Qa'ida attacks in Kenya, Saudi Arabia, and Turkey have demonstrated the group's impressive expertise to build truck bombs, and we are concerned it will try to marry this capability to toxic or radioactive material to increase the damage and psychological impact of an attack.

- We know the group has looked at derailing trains—perhaps carrying HAZMAT—to attack us.

- Al-Qa'ida has demonstrated a keen ability to use maritime assets to attack ships at berth as well as at sea. We are concerned that al-Qa'ida might employee these

techniques to attack US ships, ports, and coastal infrastructure targets such as chemical and oil facilities.

- My biggest worry, however, is how far al-Qa'ida might have progressed in being able to deploy a chemical, nuclear, or biological weapon against the United States or its allies.

We have been able to uncover important and complicated plotlines across all these disciplines and have been able to disrupt and capture key individuals involved.

But al-Qa'ida is a many-headed Hydra: regional nodes remain active—and fully capable of mounting large-scale plots, as we have seen. The terrorists we face are patient, resilient, and sophisticated. The fact that we have not seen a successful major attack against the US Homeland since 9/11 should not cause us to relax our vigilance.

Today we have an important responsibility not only to continue to educate the American people, but to put a program of security in place that is agile, seamless, and reduces our vulnerabilities without panicking our people.

- Despite our successes in stopping or disrupting attacks, the exact date, time, and place of an attack will always be elusive.

- Al Qa'ida's intent is clear. Its capabilities are circumscribed but still substantial. And our vulnerabilities are still great. Thus, in the Intelligence Community, we have to assume that more attacks will be attempted, and we have to reckon with the possibility that one of these may eventually be successfully carried out.

WHAT THIS MEANS TO YOU

Let me now turn to how these trends in the war against terrorism affect your business interests and our economic security more generally. I do so with some trepidation, knowing that in most of these areas the expertise is in the audience rather than on the podium.

As you well know, the risks and challenges faced by corporate security officers have only multiplied in the post 9/11 security environment. Undoubtedly much of your immediate focus post 9/11 has been on physical security as you endeavored to assure corporate boards, personnel, and shareholders that terror-related risks to personnel and facilities—at home and abroad—were identified and that actions had been taken to mitigate those risks.

Yet even before 9/11, corporate risks were mounting as globalization, deregulation, outsourcing, just-in-time inventory practices, and increasing use of information technology and the Internet brought greater openness and efficiency, along with new vulnerabilities.

- The change in priority security concerns is illustrated by a Pinkerton survey of the largest US firms. In 2001 firms ranked workplace violence as the main security threat, followed by Internet security and employee screening, while terrorism ranked a lowly 17th. In 2003, terrorism jumped to third place as the most pressing concern for the largest US corporations, although workplace violence remains the leading worry.

- The President's Council of Economic Advisers has estimated that private business spent an estimated $55 billion a year on private security before Sept. 11th; since then some experts forecast that corporate America may have to increase that spending by 50 to 100 percent.

- In the global economy, a security vulnerability could be a headquarters office or a factory gate, but also a computer network connection that could be a gateway to exploit a firm's databases, product designs, financial information, or personal information for identity fraud.

I have already detailed the terrorist threat and feel it is important to point out that according to State Department statistics, more businesses are targeted in terrorist attacks than all other types of facilities combined. US interests both abroad and at home, as well as US citizens working abroad, are prime targets for terrorist groups seeking to damage the US economy and affect our way of life. High-profile facilities

such as nuclear power plants, oil and gas production, and export and receiving facilities remain at risk; moreover al-Qa'ida and other terrorist groups' targets and methods may be evolving.

- Private sector cooperation is essential to protecting US critical infrastructure because nearly 90 percent is privately owned—from shipping and banking to nuclear power production, food processing, and chemical manufacturing.

- The increased number of kidnappings in the Middle East attributed to terrorist groups—a long established tactic in Latin America—may point to a new strategy to ransom the release of captured foreign combatants in US custody. US engineers working in foreign oilfields and other industrial projects could be particularly at risk.

- Shipping experts suggest that ports and maritime industries worldwide are increasingly at risk. Evidence indicates that terrorist groups have taken note of the value and vulnerability of the maritime sector, including the cruise ship industry.

At the same time the costs of mitigating these risks have skyrocketed, particularly for large multinational companies.

- The September 11th attacks inflicted the biggest single loss— currently estimated at $50 billion—ever sustained by the global insurance industry. A survey conducted by the Conference Board after September 11th found that insurance costs had risen on

average 33 percent since 2001, while costs for 20 percent of companies surveyed had doubled.

FINANCIAL THREATS

We have heard a lot about terrorists' financial networks since 9/11, but there are other financial threats that should concern us. Money laundering may not be much in the news these days, but narcotraffickers, organized criminal gangs, and corrupt leaders from around the world continue to move tens of billions of dollars into the international and US banking systems and securities markets every year. Not only does money laundering make crime profitable, the huge flows of illicit funds can undermine the integrity of individual banks, distort economies, and fuel insurgencies, such as the Revolutionary Armed Forces of Colombia (FARC).

Rogue states also engage in a wide array of illicit financial activity. They use financial cutouts to covertly acquire the goods and services needed to build weapons of mass destruction. They hide money abroad; they use front companies to beat UN sanctions with surprising ease.

Saddam Hussayn's regime amassed one of the most sophisticated illicit financial networks. It earned several billion dollars from oil smuggling and in kickbacks paid by companies that participated in the UN's "oil-for-food" program. It had covert bank

accounts, front companies, and investments scattered throughout the Mideast and as far afield as East Asia, Europe, and possibly South America.

We know that the wide extent of Saddam's network, and of the networks controlled by Iran, North Korea, and other rogues, means that numerous legitimate firms become unwittingly involved in supplying these states. The components of the network may look innocuous—a European bank or a firm run by a Singaporean businessman. In fact, increasingly they do, which can make it tough to spot the purchaser who's really helping Kim Chong-il buy a proscribed good, or the investment advisor who wants to hide Kim's nest egg.

It should also be apparent that illicit financial activity can threaten the integrity of the global financial and business system. We've seen major banks collapse because their officials were involved in money laundering, theft, and other crimes. BCCI—the Bank of Credit and Commerce International—is the "poster child," but we've seen a number of smaller banks fail for similar reasons, and several Chinese banks have suffered huge losses because of corrupt "sweetheart" loans. Cleaning up bad banks is a major goal of the US-led Financial Action Task Force. As the world grows more interconnected, the ripple effect from problems in traditional havens for illicit finance is becoming of increasing concern.

We are particularly concerned about the security of rapidly spreading electronic financial activity. The Internet has spawned a host of on-line gambling systems, banks, and

other businesses that can facilitate money laundering and covert movement of money. We've already seen a pioneer Internet bank in Aruba collapse, after it was determined to be a front for money launderers and embezzlers. We're also seeing on-line casinos set up in money laundering hubs.

Not all the threats to corporate interests are linked to terrorism or illicit finance. Intellectual property rights protection is another concern. Strong, effective IPR protection is critical to innovation, investment, and the long-term growth of the US and global economy. Unfortunately, enforcement of IPR rules around the world is lacking, particularly in developing countries. As a result, the risk of theft of intellectual property or proprietary information continues to be a large and growing problem for multinational corporations. The US Trade Representative has identified counterfeiting of trademarked goods as an increasing problem in many countries, including China, Paraguay, Poland, the Philippines, Russia, Vietnam, and Turkey.

Likewise, while outsourcing of business functions is a growing trend that helps firms cut costs, it also brings potential security risks—particularly when outsourcing involves entities owned and operated abroad.

- As many as 3 million software industry jobs could move offshore by 2015, with 70 percent of these jobs moving to India, 20 percent to the Philippines, and 10 percent to China.

- Corporate leaders need to be on guard and know who their business partners are and what security measures they have in place to protect against loss, whether through unintended leakage of proprietary business information, deliberate theft of intellectual property, or outright economic espionage.

- Technology now allows companies to have their most sensitive proprietary computer code written overseas. The inability of companies to sufficiently vet the personnel involved in these activities can create a significant vulnerability.

US openness to foreign trade and investment and our commitment to global information sharing through academic and scientific exchange unfortunately also leave our technologies highly exposed to foreign exploitation.

- Collectors last year employed a wide variety of techniques in their quest to circumvent US restrictions in the acquisition of sensitive technologies—not only militarily critical technologies but manufacturing processes, biometrics, and pharmaceuticals, to name just a few.

- Naturally, the simplest, safest, and least expensive methods were the ones most widely used. In a surprising number of cases, foreigners—often through middlemen—acquired sensitive US technologies simply by requesting them via e-mail, faxes or telephones.

CYBER THREATS

Globally networked information systems also present vulnerabilities, and even the simplest computer threats pose real risks for your companies' business interests and proprietary knowledge. Some of you may even have personal experience with these threats from your international travels and business dealings: a laptop computer or Palm Pilot stolen at a conference, in an airport, or from your hotel room.

- We have seen foreign intelligence services make use of many such venues, sometimes more subtly than outright theft: Hard disks, CDs, and other media can be copied and then quickly returned. The hacker underground studies the art of computer intrusions with no physical tethers at all, scanning computers with wireless network capabilities for access holes to slip through.

No country in the world rivals the United States in its reliance, dependence, and dominance of information systems. The great advantage we derive from this also presents us with unique vulnerabilities. Rapid changes in technology, the integration of telecommunications and computer networks, and increasing dependencies of traditional infrastructure elements on digital networks create avenues for access that attackers can exploit before defensive measures can be devised. At the same time, Internet-available hacker tools, now more sophisticated and accessible, have matured from being a source of nuisance to a credible and serious attack threat.

The vulnerabilities to US national and economic security as a result of increasing US dependency on foreign IT hardware and software design and manufacture, outsourcing, knowledge transfer and globalization, are significant.

- Information technology has become as important to the US economy as oil, and the growing dependency of the US on foreign IT raises concerns for corporate as well as national security. For example, half of the world's laptops, one quarter of all desktop computers, and half of all PC motherboards are now assembled in China. Taiwan is now responsible for about 70 percent of all semiconductor production for hire—producing chips designed and marketed by others.

- This growing US dependence makes US IT firms vulnerable to interruptions of foreign-built critical components, whether intentional or accidental. Foreign supply disruptions could suspend US firms' deliveries of finished systems within only a few days as most carry limited inventories.

Advanced technologies and tools for computer network operations are becoming more widely available, resulting in basic, but operationally significant, technical cyber capability for US adversaries.

The majority of malicious software that has caused some damage and disruption to US infrastructure has not used the most advanced or targeted techniques. In most cases,

the malicious software takes advantage of vulnerabilities that have simply gone unpatched. A couple of the most significant recent examples include:

- ***Slammer—Winter 2003***. Slammer worm's rapid propagation resulted in a flood of spurious network traffic and many reports of disruptions. According to industry experts, within the first 10 minutes, Slammer had infected 90 percent of all vulnerable computers worldwide. At its peak, Slammer displaced 20 percent of Internet traffic—an impact that matches the most disruptive viruses and worms to date.

- ***Bugbear—Spring 2003***. Bugbear—one of the first worms to target a specific group—is designed to extract information from victims' computers that may be used for future theft, extortion, and disruption. It attempts to steal passwords from bank employees associated with a pre-composed list of 1,200 financial institutions, and its targeting may result in back-office operations access, where more valuable transactions occur.

Whatever direction the cyber threat takes, the United States will be confronting an increasingly interconnected world in the years ahead. As a recent CIA report points out, a major drawback of the global diffusion of information technology is our heightened vulnerability. Our “wired” society puts all of us—US businesses, in particular, because you must maintain an open exchange with customers—at higher risk from enemies. In general, IT’s spread and the growth of worldwide digital networks mean that we are

challenged to think more broadly about national security. We should think in terms of global security, to include the dawning reality that freedom and prosperity in other parts of the world are inextricably bound to US domestic interests.

TERRORISM'S ROOT CAUSES

I referred earlier to the "war on terror," but war is a poor metaphor, or at least an incomplete one. In some respects this surely is a war. But the struggle against terrorism, as I have outlined it today, has many facets. Some dimensions can only be addressed by governments; others fall to the private sector.

If this is a war, it is a war that cannot be "won" in any final sense, but only attenuated, contained, managed. Terror is the tactic, not the adversary itself. To deal with these threats over the longer-term we have to deal with underlying causes:

…like the numbers of societies and peoples excluded from the benefits of an expanding global economy, places were autocratic rulers rig politics and economies for their own benefit, where the daily lot may be hunger, disease, displacement, where young people grow increasingly disaffected and believe that radical solutions are the last remaining choice.

- Large areas of the world are becoming hard-to-govern lawless zones—veritable no man's lands—where extremist movements may find the breathing space to grow and new safehavens are created.

Let me explain this in more detail.

Imagine a large map of the world. Let's say we stick a map pin in **every country** that had a **low per capita income**. And another for a **high rate of infant mortality**. Another for a **sizable "youth bulge**"—what Robert Kaplan calls "unemployed young guys walking around"—a strong indicator of social volatility. And another pin to mark an absence of political freedoms and participatory government.

- At the end of this exercise, we would have marked out a large number of vulnerable states—many in the Muslim world.

We could go on to mark out another set of what we could call "beleaguered states"—states unable to control their own borders and internal territory, that lack the capacity to govern, educate their peoples, or provide fundamental social services.

We end up with a map full of pins and many states with more than one. We know from experience that states struggling with these problems are the natural targets of the terrorists. We've seen—in places like Afghanistan—terrorists gaining a foothold and turning them into terrorist havens.

Now consider this:

An estimated **1 billion people worldwide remain chronically malnourished** today. The vast majority live in 70 low-income food-deficit countries.

- This is despite an improved global food picture—steady increases in world grain production, falling real food prices, and rising incomes in key developing countries, such as China and India.

Meanwhile, during the last year **3 million people died of AIDS**.

- By 2010, as many as **100 million HIV-infected people** will reside outside of Africa. China could have 15 million cases and India between 20 and 25 million—more than any other country in the world.

- AIDS encourages the spread of **tuberculosis**, including drug-resistant strains. And **malaria** kills almost a million Africans per year, mostly children.

- The **national security implications** are staggering. Disease honors no border, will undermine economic growth, diminish military readiness, and further weaken beleaguered states—creating great opportunities for extremists to exploit. And, it will affect the multinational work forces you will need to hire to run your businesses.

By 2007, for the first time in human history, **a majority of the world's population will live in cities**. High urban population densities in economies that are not growing go hand-in-hand with acute problems of governance, highly uneven income distribution, and ethnic and religious tensions.

- In the next 15 years, the global population will grow by 1.5 billion people, mostly in Asia and Sub-Saharan Africa.

As for the destabilizing **"youth bulge,"** of the 54 countries with large **Muslim populations**, 21 are currently contending with large numbers of unemployed young people.

- Half the Saudi population is under the age of 15.

"Globalization," which brings tremendous benefits to societies able to participate, is nevertheless creating **new classes of haves and have nots**. For all its advantages, globalization can also contribute to unequal growth and highly skewed income distributions. According to the World Bank:

- In **Honduras**, the richest fifth of the population receive about 38 times as much as the poorest quintile. In **Bolivia**, the top quintile receive 32 times the lowest.

Contrast these to **Japan or Austria**, in which the top fifth earns just about three times more than the lowest. (In our own country, the ratio is about 14/1.)

If you want a recent dramatic example of the potentially destabilizing effects of widespread poverty amid a high concentration of wealth, look no further than Bolivia and the forced resignation of former President Sanchez de Lozada. (I might add that the mobilization of the Inca population is itself a phenomenon that would have been hard to imagine just a few years ago, before globalization took hold.)

We also have to reckon with reactions to US preeminence around the world——as other countries and peoples adjust to a world with a single superpower—and with a sharp rise in anti-Americanism, especially (but not only) in the Arab Middle East.

We are already seeing some backlash against the US economic model that will surely complicate business relations. Indeed, many accuse the United States of defining the rules in the international system to favor its own cultural propensity. The situation can become particularly dangerous for US business when cultural resentments against the United States are used to legitimatize economic resentments.

- The United States' "pure" form of capitalism—allowing companies to die and then reallocating capital to more "efficient" organizations—already is creating a perception of US callousness that enhances tensions between the United States and other

cultures. For many, equality, distributive justice, and social harmony are just as important as how politics and society are organized.

Animosity against the United States and US interests is unlikely to dissipate over time. For example, the emerging generation in many countries has a stronger sense of nationalism than predecessor generations; this trend, even in democracies, could unleash xenophobic policies harmful to US interests.

AN AGENDA FOR THE FUTURE

Let me mention a few ways in which we are trying to address these new strategic challenges. Within the NIC, we have just created a new NIO account to deal with transnational threats, including terrorism—not to duplicate the work of the many organizations dealing with day-to-day counter-terrorist work, but to look over the horizon at broader trends that day-to-day operators may miss.

- For example, we know that failed states can offer safe havens for terrorists. But which states will fail, and which of those will in fact be attractive sites for terrorists?

- Also, we need to monitor global trends in political Islam—not all of which are associated with terrorism, let me hasten to add.

- What about other sources of global terrorism? Will Leftist terrorism, which virtually disappeared from Europe after the disbanding of the Red Brigades and the Bader-Meinhof gang, make a comeback? Will class-based terrorism make a revival in Latin America?

On these and many other issues, we must look outside government to find the expertise on which we must draw. Here the NIC can play a critical bridging role between outside experts and policymakers. Having spent a career going back and forth between these two worlds, I see this as one of the principal roles I can play.

Toward that end, the NIC just launched an ambitious, yearlong project called NIC 2020, which will explore the forces that will shape the world of 2020 through a series of dialogues and conferences with experts from around the world. For our inaugural conference, we invited 25 experts from a wide variety of backgrounds to join us in a broad-gauged exploration of key trends.

- These included prominent "futurists"—the longtime head of Shell's scenarios project, the head of the UN's millennium project, and the director of RAND's center for the study of the future.

- Beyond that, we had experts on biotechnology, information technology, demography, ethnicity, economic development, and energy, as well as more traditional regional specialists.

Later on we will be organizing conferences on five continents and drawing on experts from academia, business, government, foundations, and the scientific community, so that this effort will be truly global and interdisciplinary. We will commission local partners to convene these affairs and help set them up, but then we will get out of the way so that regional experts may speak for themselves in identifying key "drivers" of change and a range of future scenarios.

- As the 2020 project unfolds, we will be posting discussion papers, conference reports, and other material on our unclassified Web site, so I encourage you to follow the project as it unfolds over the coming year.

It may seem somewhat self-indulgent to engage in such futurology at a time of acute security challenges, but I see this as integral to our work. If we are entering a period of major flux in the international system, as I believe we are, it is important to take a longer-term strategic review.

We are accustomed to seeing linear change, but sometimes change is logarithmic: it builds up gradually, with nothing much seeming to happen, but then major change occurs suddenly and unexpectedly.

- The collapse of the Soviet empire is one example.

- The growing pressures on China may also produce a sudden, dramatic transformation that cannot be understood by linear analysis.

As I used to say to my students, linear analysis will get you a much-changed caterpillar, but it won't get you a butterfly. For that, you need a leap of imagination. I hope that the 2020 project will help us make that leap, not to *predict* the world of 2020—that is clearly beyond our capacity—but to *prepare* for the kinds of changes that may lie ahead.

I have said a few words about our agenda. But let me add that we have a lot to learn from you. So while I have enjoyed this opportunity to speak and look forward to your questions and comments, I hope the dialogue between business and government will be ongoing – through national and international organizations like ISMA and the State Department's Overseas Security Advisory Council, in local contacts with the Joint Terrorism Task Forces, and in regular contacts at all levels.

Thank you for your attention. I look forward to your comments.