



Viewpoints contain background analyses and comments on critical global and regional trends, issues and developments. *Viewpoints* also occasionally include analytical reviews of ISEAS books. The responsibility for facts and opinions expressed rests exclusively with the authors and their interpretations do not necessarily reflect the views or policy of ISEAS.

A Time Bomb for Global Trade: Maritime-related Terrorism in an Age of Weapons of Mass Destruction.

By Michael Richardson

This summary report is EMBARGOED. It is not to be published or broadcast before 8pm Singapore time (noon London/7am New York/Washington) on Wednesday 25 February, 2004.

PREFACE

This report aims to answer these questions:

- 1) Are Al-Qaeda, the world's most feared terrorist network, and like-minded extremist groups interested in using ships, ports, and the sea and land links in the global cargo container supply chain, for their own purposes?
- 2) Is one of their aims to use a ship or container as a weapon to attack a major port-city or disrupt traffic in a key strait or waterway for international shipping, possibly using a nuclear or radiological bomb?
- 3) If so, could such an attack slow or even halt seaborne trade, a vital engine of the world economy?
- 4) What is being done to counter threats and how effective are the safeguards?

These questions may sound melodramatic. But the evidence gathered in this report shows that the threats to seaborne trade and its land connections, including ports and adjacent cities, are very serious and are being treated as such by knowledgeable officials, private sector executives and security analysts in North America, Asia, Europe and Australasia whose countries, trade, assets and people abroad may become terrorist targets.

Much is now known about the operations and plans on land and in the air of Al-Qaeda, its affiliates and emulators. This has been widely publicised. But less is known about the maritime-related activities of terrorist organisations and the report documents them. Governments around the world are concerned not only that Al-Qaeda and like-minded terrorist groups will strike more frequently, but that they may strike with more powerful weapons in new ways, including via the sea.

As this report makes clear, the Al-Qaeda network aims to disrupt the seaborne trading system, the backbone of the modern global economy, and would use a crude nuclear explosive device or a radiological bomb to do so if it could get its hands on either and position it to go off in a port-city, shipping strait or waterway that plays a key role in international trade.

The report does not cover chemical or biological weapons, although both are of interest to Al-Qaeda and other extremist groups. While terrorists might use ships or cargo containers to smuggle chemical or biological weapons or poisons into a country for an attack, these toxins could not be effectively dispersed by ship or container and would need to be offloaded for final use. By contrast, terrorists with nuclear or radiological bombs that were brought to their target by sea would use the ship or container to hide, deliver and detonate the device.

This report does not deal with the risk of terrorists attacking cruise liners or offshore oil or gas fields and installations. Both are a real possibility and could cause many hundreds of casualties and much localised damage. The risk for cruise liners has been obvious since the Achille Lauro was hijacked by Palestinian terrorists in 1985. But neither of these maritime terrorism possibilities has the potential to disrupt world trade unless a cruise liner was sunk, scuttled or exploded in the way this report defines for other ships involved in a mega-terror plot.

THE REPORT IN SUMMARY

Given the vast scale of the global shipping and cargo container industry and its vulnerability to acts of terrorism, better security is vital when the risk of weapons of mass destruction reaching international terrorists is rising. Improving maritime security is especially important for the United States and Canada, member states of the European Union, Australia and New Zealand, and for China, Japan, South Korea, Taiwan, Thailand, Malaysia and other economies in East Asia that have extensive direct seaborne trade with the US, Europe and other industrialised nations. It is doubly vital for places like Singapore, Hong Kong and Rotterdam that are not only very large seaports with global connections, but also giant container transshipment hubs.

Asia-Pacific Stake

China and many other Asia-Pacific economies that have industrialised rapidly in the past few decades depend heavily on seaborne trade. Asia controls and operates more than 40% of the global commercial fleet, supplies the vast majority of its crews and builds most of its ships. Many of the world's biggest ports are in East Asia and much of the traffic they handle passes through the key straits of Southeast Asia.

Over a quarter of the world's trade and half its oil go through the Straits of Malacca and Singapore. The energy and raw materials that traverse Southeast Asian straits keep the economies of Japan, greater China and South Korea humming. Without these reliable seaborne supplies, the Northeast Asian regional economy would slow drastically, if not grind to a halt. Much of Australia's trade is with East Asia and goes by sea through Southeast Asian straits. The Asia-Pacific stake in maritime security is therefore huge.

Post-9/11 & Terrorism

On 11 September 2001, Al-Qaida used hijacked civilian jet airliners as weapons to kill nearly 3,000 people. Two of the planes were flown into the World Trade Center twin towers in New York, bringing both skyscrapers down. Another of the hijacked airliners crashed into the headquarters of the US Defence Department in Washington. They were stunning strikes on the centres of financial and political power in the US.

The use of hijacked civilian airlines as cruise missiles to strike New York and Washington fundamentally changed the way security is approached in the transport sector. It exposed a whole new degree of vulnerability in the global transport system. Following the attacks, the US closed its air space for four days and its ports for two days. Border crossings were closed along the frontier with Canada, where half a million vehicles cross daily, leading to severe logjams. Some companies dependent of just-in-time deliveries experienced a breakdown in their supply chains. New security measures were introduced, initially for aviation but later for other forms of transport as well.

The Bush administration has poured billions of dollars into tighter airline security, mainly to improve checks of passengers and their baggage. Some US officials fear that the next big attack on America could come by sea, not by air. Many officials in Asia, Australia, New Zealand and Europe share this concern about maritime-related terrorism. Al-Qaeda has said a number of times that it wants to shut key searoutes to strike a mortal blow at the political economy of the West.

So far, terrorists have mainly used trucks and other motor vehicles packed with explosives or fuel-laden aircraft as their most destructive weapons. Now, one of the biggest concerns of authorities is that terrorists may strike using another vital form of transportation – ships and cargo containers.

Officials and counter-terrorism experts in the US, Europe, Asia, Australia and many other parts of the world have warned that the next step up in mega-terrorism may be an attack using chemical, biological or nuclear weapons or, more likely, a radiological or “dirty” bomb that uses conventional explosives to disperse deadly radioactive material, causing mass panic as well as significant casualties. Some say that a dirty bomb attack is inevitable sooner or later.

Those who fear such an attack believe that weapons of mass destruction and terrorism have become interlocking threats – and could, if effective safeguards are not put in place quickly, fuse in an extremely dangerous challenge to global security and stability. The recent exposure of an extensive and long-running nuclear black market

that let Iran, Libya and North Korea get weapons technology from Pakistan has heightened such fears.

The Labyrinth World: Shipping and containers

Shipping plays a pivotal role in world trade. Most international trade – about 80% of the total by volume – is carried by sea. World maritime trade set a record in 2002, reaching almost 5.9 billion metric tons, including oil and bulk commodities, and general cargo packed mainly in containers. This commerce is worth at least \$US 1 trillion a year. About half the world's trade by value, and 90% of the general cargo, is transported in containers - standardised steel boxes that are usually 20-foot or 40-foot long, and are commonly referred to as “twenty-foot equivalent units” (TEUs) or “forty-foot equivalent units” (FEUs).

This is an industry of vast scale and labyrinthine complexity. But the global shipping industry is not only vast; it is poorly regulated, frequently beyond the reach of the law and often secretive in its operations, especially in concealing the real owners of ships. Oceans cover two thirds of the world's surface and most of this huge area is classified by law as international waters, or high seas, where ships are free to roam unhindered except in certain very specific circumstances. Despite a raft of new anti-terrorist measures that took effect in 2002 and 2003 and more that will be applied in 2004, the sea and the shipping industry remain an attractive domain for terrorist operations.

The Seafarers' Free-for-all

Most seaborne international trade is carried by at least 46,000 ships calling at over 2,800 ports. There are more than 1.2 million seafarers and hundreds of thousands of port workers.

Al-Qaida and its international affiliates could with relative ease infiltrate the ranks of seafarers, most of them sourced from Asia, Eastern Europe and Russia. Demand for the relatively highly paid jobs in seafaring exceeds supply. Regulation of recruitment and manning practices is lax. As a result, fraud and corruption are rife. Research in the past few years has shown that a large number of qualification certificates held by seafarers are fraudulent and that fake papers for crew members can be bought and sold easily.

For example, in 2001, the International Transport Workers' Federation said that it had bought a First Officer's certificate for its General Secretary, David Cockroft, who is a “landlubber” with no shipboard training or experience, from Panama which operates the world's largest ship register. The ITF said it paid \$US4,500 for the certificate and seaman's book that authorised Cockroft to navigate a vessel and deputise for its captain, despite his complete lack of marine qualifications and skills. The ITF says that fake certificates remain a problem.

Seafarers have traditionally been granted relatively liberal landing and travel rights by governments when they present their seafarer identity documents. Since 9/11, the Bush administration has imposed restrictions on seafarer movement in the US. A significant proportion of the world's commercial fleet gets crews from

manning agencies that match candidates with the requirements of ship owners and operators. While many of these agencies are reputable and ensure that the seafarers they represent fulfil international requirements and pass background checks, some do not.

In such a situation, there is considerable scope for terrorists to pose as crew and then take over a ship to use it as a weapon of attack. Many large modern ships are highly automated and can be operated by crews of well under 20 officers and ratings. So it would only take a small number of well-trained and determined terrorists to seize command of a big ship.

The Container Supply Chain Maze

Apart from ships and ports, the millions of uniform steel containers that carry most of today's general cargo around the world are a security nightmare. Once loaded and sealed, inspection is a problem. The contents of a container can be misrepresented and undeclared items hidden inside with relative ease. Even when sealed, containers can be surreptitiously opened and then closed again without great difficulty to remove or add contents. This is a made-to-order method of transport for terrorists – just as it is for drug and other contraband smugglers.

It is estimated that as many as 15 million containers are in circulation and that over 230 million containers move through the world's ports each year. Nearly seven million containers arrive by sea in US ports alone each year. They carry goods worth more than \$US 730 billion. Checks of containers reaching American ports by sea increased to 5.2% of total arrivals by September 2003, from 2% two years earlier. But worldwide, less than 1% of shipped cargo is screened.

Sea-Land Links in the Global Supply Chain

Like the seaborne trading system, the global supply chain is vast, complex and vulnerable to terrorist infiltration and attack. There are some 40,000 freight forwarders worldwide who employ as many as 10 million people.

While most of the world's trade travels by sea, the ocean voyage is only one link in an extensive chain. A typical door-to-door journey for general cargo in a shipping container will involve some 25 different handlers, generate up to 40 different sets of documents, use several other transport modes like truck or rail, and pass through as many as 15 different locations, from the factory or warehouse where the goods are loaded into a container, to the point of unloading and delivery.

Secure Trade v Free Trade

The very nature and scale of the globalised trading system makes it vulnerable to terrorist attack. Seaborne trade and its land connections in the global supply chain have become increasingly open. They are liable to be targeted or exploited by terrorist groups that have the capability to strike in different parts of the world and aim to cause as much fear and chaos as possible to advance their ends.

In recent decades, the Asia-Pacific region has followed its main trade partners in North America and Europe in deregulating and encouraging freer trade and commerce, to foster economic growth. In the wake of the terrorist attacks on the US in September 2001, and the subsequent plots and bombings in Indonesia and other parts of Southeast Asia, the region and its leading trade partners must tighten security at sea, in ports and throughout the logistic supply chains that have become critical to modern manufacturing and service industries.

The global economy is built on integrated supply chains that feed components and other materials to users just before they are required. That way, inventory costs are kept low. If the supply chains are disrupted, it will have repercussions around the world, profoundly affecting business confidence at a time when economic recovery is still tentative and the outlook uncertain.

On the other hand, if security measures start to slow global trade significantly or make it much more expensive, the world economy will suffer. Striking the right balance between free trade and security is critically important, and it must be done in 2004 as a wide range of new counter-terrorist measures take effect.

Benefits of Secure Trade

However, the new security measures, when effectively applied and extended on a more universal basis, could help streamline global commerce as well as make it more secure. The benefits, which can amount to significant savings, should include faster processing when containers reach US ports, lower insurance costs and fewer losses due to theft. The security requirements will make it more difficult to falsify the identification of goods for customs declaration purposes. This will reduce the scope for corruption and cut transaction costs.

For example, the estimated losses from cargo theft worldwide range from 30 billion US dollars per year to as high as 50 billion dollars, with most of the thefts involving cargo containers being transported by trucks. However, seaports and container staging areas are also prone to containerised cargo theft. The installation of container scanners in the Port of Rotterdam cost 15 million Euros. But in one year, their use generated 88 million Euros in customs and tax revenue that would otherwise have been lost, even though only 2% of containers, on average, are subjected to checks in the port.

One of the greatest potential benefits of the US-led drive to make container shipments more secure is the technology innovation it is spurring as governments and the private sector, increasingly in collaboration, seek new ways to overcome problems raised by fears of terrorism. A global seaborne transport system and supply chain network that are made more secure by advanced technology would be an enormous boon to trade, business and job creation.

Multinational companies and other trade-reliant firms have a vested interest in hastening this result because they do not want any interruption in the supply chain that would keep their goods out of world markets and cost them money. Even those who worry about the costs of meeting the new security requirements, acknowledge that the

potential damage from a major terrorist attack using ships or cargo containers could be many times higher than the costs of enhanced security.

Containers

Vessels, big and small, or the cargo containers they carry can be used in a number of ways by terrorists to further their aims:

...to raise money, through legal or illegal trade, to finance their activities;

...to covertly transport operatives, equipment and weapons to provide support terrorist operations;

...to deliver bombs or other means of destruction to their destination, such as in a container set to explode near a port-city or other target;

...to use vessels as weapons in their own right. Oil and chemical tankers could be sunk or set ablaze in a busy strait, waterway or port to cause pollution and disrupt shipping. Ammonium nitrate carriers or petroleum tankers could be rigged as floating bombs. Ammonium nitrate is a common agricultural fertiliser. It is widely traded around the world by sea. But it can, when mixed with fuel oil, be turned into a powerful explosive. Packed into trucks, vans and cars, it has been used in many terrorist bombings.

Terrorists and Sea Transport

The terrorist network linked to Al-Qaeda understands the vital role of sea transport and has exploited it for many years. For example, one Al-Qaeda vessel delivered the explosives that its operatives used to bomb two US embassies in East Africa in August 1998, killing 224 people. Nearly all were Africans. But 12 Americans were among the dead. In December 2003, US and allied forces on patrol in the Persian Gulf tracked and boarded several dhow trading boats, confiscating three drug shipments worth more than \$US 15 million. US officials said that seven of the 45 crewmen detained had links to Al-Qaeda and the organisation was using drug smuggling to help finance its operations.

Al-Qaeda has used cargo containers to ferry agents and probably terrorist-related material around the world. Shortly before he was captured in Pakistan in March 2003, Al-Qaeda's director of global operations Khalid Shaikh Mohammed was involved in a plot to use containers that shipped garments from Karachi to New York. The Director of the US Central Intelligence Agency George Tenet has described Khalid Shaikh Mohammed as "the mastermind" of Al-Qaeda's airborne attacks on the US in September 2001. According to court documents prepared by US government prosecutors, Al-Qaeda's number 3 man, after Osama bin Laden himself and his deputy Ayman al-Zawahri, offered to invest US\$200,000 in the garment business in exchange for access to its shipping containers bound for Port Newark in the New York-New Jersey harbour complex.

Trojan Box

The fear that terrorists could exploit the container transport system was confirmed barely a month after the Al-Qaeda hijackers crashed civilian airliners with their passengers into the World Trade Centre twin towers and the Pentagon.

In October 2001, authorities in the southern Italian port of Gioia Tauro discovered an unusually well-equipped and neatly dressed stowaway locked inside a shipping container. It was furnished as a makeshift home with a bed, water, supplies for a long journey and a bucket for a toilet. Italian police named the stowaway as Rizik Amid Farid, 43, and said he was born in Egypt but carried a Canadian passport. Unlike most stowaways, he was smartly dressed, clean-shaven and rested as he emerged. He was found to be carrying two mobile phones, a satellite phone, a laptop computer, several cameras, batteries and, ominously given recent events in the US, airport security passes and an airline mechanic's certificate valid for four major American airports.

Gioia Tauro is a leading trans-shipment hub for cargo in the Mediterranean. The container fitted out as a makeshift home had been loaded in Port Said, Egypt. Had the stowaway not been trying to widen ventilation holes when workers in Gioia Tauro were nearby, the box may well have passed unhindered to its final destination at the port of Halifax in Canada, via Rotterdam in Holland. After he was discovered, Farid was investigated by Italian prosecutors who suspected he was an Al-Qaeda operative. Farid was charged with illegal entry into Italy and detained. But a court released him on bail and he disappeared before further information about him and the purpose of his unorthodox means of travel could be gathered.

Al-Qaeda's Maritime Operations

Al-Qaeda and other terrorist groups, including the Tamil Tiger guerillas in Sri Lanka, have used ships to make money in legitimate and illicit trade, and to smuggle operatives, arms and supplies. They have also used small boats laden with high explosives to sink or severely damage much larger and more modern ships. Al-Qaeda used this method successfully in October 2000 in Aden harbour, Yemen, against the American destroyer USS Cole, nearly sinking one of the US Navy's most sophisticated warships. Two years later, a similar tactic was used to cripple and set ablaze the French-registered oil tanker, Limburg, carrying crude oil off the coast of Yemen, Osama bin Laden's ancestral birthplace.

Al-Qaeda's former chief of naval operations, Abdul Rahim Mohammed Hussein Abda Al-Nasheri, captured in Yemen in November, 2002, has given CIA investigators information that reinforces concerns about plans for terrorist attacks against shipping. Al-Nasheri has reportedly admitted playing a key role in organising the attacks on the USS Cole and the Limburg.

Al-Nasheri, nicknamed the Prince of the Sea, is also said to have confessed to planning attacks on shipping in the Strait of Gibraltar. Early in 2002, Al-Nasheri sent a team of several Afghan-trained Saudis to Morocco to prepare for bomb-laden speedboat attacks on US and British warships as they passed through the strait between the Mediterranean Sea and the Atlantic Ocean. Morocco is just 12 miles from Gibraltar across the strait. The Moroccan intelligence service foiled the plot but a key operative escaped.

Anti-terrorist investigators worry that divers trained by Al-Qaeda or its affiliates could plant explosives on the hulls of ships or act as seagoing suicide bombers. But professional divers with military experience say that mounting a successful underwater attack against a ship or offshore installation would be more difficult than attacking it with an explosive-laden boat. Underwater strikes require specialized equipment, training and explosive charges.

Jemaah Islamiyah's Maritime Terrorism Plans

The Singapore government has said that when it cracked down on the Jemaah Islamiyah network in the island-state starting in December 2001, it discovered that the group had made preliminary plans to prepare for suicide attacks on US warships visiting Singapore. JI's plans to mount multiple ammonium nitrate truck bomb attacks against Western and Israeli diplomatic and other targets in Singapore, including naval bases used by the American military in Singapore, were more advanced.

The plans to attack US warships with explosive-laden small boats manned by foreign suicide bombers were started from around the mid-1990s and were fairly well developed, although never activated.

The planning for the attack on the USS Cole in Yemen in October 2000 reportedly began in Malaysia. One of the key suspects - Tafiq Muhammed Saleh bin Roshayd bin Attash, also known as Khallad - is said by US officials to have directed the Cole attack with Al-Qaeda maritime commander Al-Nasheri. Attash was plotting another attack on a US ship visiting a Malaysian port in 2000. Less than a year later, Malaysian intelligence foiled a plan to attack a second US ship.

Maritime-related Terrorism: Still a Serious Threat?

Since the terrorist attacks on the US in 2001, many Al-Qaeda leaders have been captured and the organization's financial system, communications networks and training camps in Afghanistan disrupted.

In Southeast Asia, Al-Qaeda's closest ally, the JI, has also been hounded by tougher law enforcement and better intelligence sharing among countries in the region and between them and counterpart agencies in the US, Australia and elsewhere.

In addition, many new security measures to protect maritime trade, container cargo shipments and their land connections in the global supply chain have been implemented or will be during 2004.

How will this affect the plans for maritime-related terrorism that Al-Qaeda and its affiliates, including the JI in Southeast Asia, were trying to develop and implement? Al-Qaeda clearly had a much more sophisticated program for striking at seaborne trade and the global cargo container supply chain than JI, which so far as is publicly known had only prepared a preliminary plan to attack US warships in or close to Singapore.

The operational capability of both Al-Qaeda and JI have certainly been set back. But, given the Protean nature of the Al-Qaeda network, no one can be sure how serious a blow has been struck or how long the terrorists will take to recover and attack again. Their fight is likely to continue for a long time and take many different forms.

The capture of dozens of terrorist operatives in 2002 and 2003 in North Africa, the Persian Gulf, the Horn of Africa and Pakistan, as well as investigations into the attacks on the USS Cole and the Limburg, uncovered detailed training and planning procedures by Qaeda-linked terrorist networks specifically designed to target maritime interests. Although the arrest of some significant planners and operatives was seen as a setback to Al-Qaeda and its affiliates, the investigations revealed a terrorist network that is larger than previously thought and still capable of carrying out bombings and other attacks against maritime targets.

Building and detonating a radiological bomb or commandeering ships and using them as weapons to attack key port-cities, straits or waterways are well within the capability of Al-Qaeda and some of its affiliates. So constant vigilance must be maintained and layered defences built to guard against such an attack.

The World-wide Watch for Maritime Terrorism

US and allied or friendly navies and their intelligence agencies are constantly searching for ships owned by Al-Qaeda or their front companies or representatives that provide ready cover for terrorists in the vast and murky world of international shipping. But tracking suspected terrorist vessels is difficult.

Intelligence agents have to watch tens of thousands of merchant ships. Suspect vessels are regularly renamed, repainted and put on a different register using invented corporate owners. Hiding the ownership of ships under layers of corporate subterfuge is a legal and longstanding practice in many countries, industrialised and developing alike.

Flags of Convenience

More than half the world's seagoing fleet by tonnage is registered not in its home country on a national shipping register, but on any one of at least 40 open registers in foreign countries. This is done to cut costs, taxes and regulation and ensure anonymity for the real owners of the vessels. These so-called flag of convenience registers are sanctioned mainly by developing countries to make money. They compete for business. Some offer quick and cheap ship registration, often on-line at the click of a button with few questions asked. As a result, terrorists as well as those who smuggle arms, drugs, people and contraband can thrive in the poorly regulated havens which the flag of convenience system provides.

For example,

... in August 2001 a group of 15 Pakistani men were charged in Italy with conspiracy to engage in terrorist acts after they were taken as Al-Qaeda suspects from a freighter. The captain said that the ship's owner had forced him to take them aboard

in Casablanca, Morocco, and that they had menaced his crew. The freighter was flagged and registered in Tonga, a small island nation in the Pacific, but was owned by a Greek who operated it through a company based in Romania and the US state of Delaware.

...in November 2001, Irish customs officers found 20 million smuggled cigarettes on the Maria M, a cargo ship flying the Cambodian flag that arrived from Estonia carrying a cargo of timber. The cigarettes, concealed in the center of bales of timber, were liable to tax amounting to about three million Irish pounds. They were the largest haul of smuggled tobacco ever seized in Ireland. Anti-terrorist officials said that the operation was organised by criminals with links to the Real IRA, a terrorist faction opposed to the peace accord in North Ireland agreed to by the mainstream IRA, the Irish Republican Army.

...in December 2002, the US asked its NATO ally, Spain, to send a warship to halt and inspect a freighter from North Korea in the Indian Ocean as it steamed towards the Middle East. North Korean officials have on several occasions in the past few years threatened to export weapons of mass destruction. They already export ballistic missiles, in most cases legally. The ship was sailing without a flag or registered name, meaning that it could be boarded under international law. A subsequent check of the cargo holds by American forces found crates containing 15 Scud missiles, 15 conventional warheads and many barrels of chemicals, all hidden under thousands of bags of cement. But the US decided to let the freighter sail on to its destination, Yemen. There was no legal basis for holding the missiles and their purchaser, the Yemeni government, was an important ally of America's in the war on terrorism.

The Proliferation Security Initiative

It is against this background of significant crime and lax regulation in international shipping – and the industry's vulnerability to abuse by terrorists – that US President George Bush launched the Proliferation Security Initiative, or PSI, in May 2003. Various referred to as a compact or political arrangement, it is a program of preemptive interdiction designed to intercept illicit exports related to weapons of mass destruction anywhere in the world, whether by sea, air or land. The PSI is premised on the growing concern that countries or criminal organizations hostile to America will pass wmd-related materials to terrorists who may use them to attack the US, its allies or friendly countries around the world. North Korean shipments have been the main target of the programme so far.

There are eleven founding PSI members: Australia, France, Germany, Italy, Japan, the Netherlands, Poland, Portugal, Spain, Britain and the US. In December 2003, they were joined by five additional participants: Canada, Denmark, Norway, Turkey and Singapore. The PSI aims to expand its reach by getting cooperation from countries that have large shipping fleets and those whose ports and waters may be used by shippers of wmd-related goods. US officials say that more than 50 countries have signaled that they support the PSI and are ready to take part in interception efforts, most of which are expected to be within national jurisdiction and the result of better exchanges of intelligence and tighter export controls.

Container Security: From Extreme Vulnerability to Semi-vulnerability

To help secure container shipping trade and the global supply chain, the US has introduced a raft of new security measures, including the Container Security Initiative. The scheme is intended to prevent the use of cargo containers by terrorists, especially to hide weapons of mass destruction or radioactive materials. Most of the leading ports in Europe and Asia that trade with the US have decided to participate in the CSI. They have agreed to allow US customs officers to be stationed in their ports to work side by side with local inspectors to check containers bound for the US.

But this report shows that despite new safeguards, maritime and container cargo security is still open to abuse by terrorists. The global system has moved from a position of extreme vulnerability two years ago, to one of semi-vulnerability while new counter-terrorist measures are implemented and bedded down and more powerful and effective technology is applied to thwart terrorist infiltration or attacks. This could take at least several more years to be fully developed and widely applied at an affordable cost. Meanwhile, radiation detectors and X-ray machines at major ports in North America, Europe, Asia and Australia and New Zealand are good and getting better. But neither they or their operators are foolproof.

Given the huge scale of maritime trade and the even vaster scale of commerce moving through the global supply chain using cargo containers, the task of applying tighter security from the point at which containers are loaded and sealed to the point at which they are unloaded is difficult and far from complete.

For the time being, accurate and timely intelligence of any terrorist threat is the key to success. But those looking for signs of weapons of mass destruction or radiological substances among the many millions of containers moving around the world carrying legitimate cargo are checking for the proverbial needle in the haystack. And they are under constant pressure to do so without unnecessarily slowing global trade or increasing its cost.

This period of semi-vulnerability to a catastrophic terrorist attack could last for at least several more years if – as appears likely – not all companies and countries move with the same speed or effectiveness to tighten security at ports, on ships and in the global container cargo supply chain. Overall security will only be as good as the weakest link in the chain.

The Nightmare

The most dangerous possibility in maritime terrorism – indeed it is a nightmare scenario for many officials and analysts in the West and Asia – is that terrorists might sooner or later get and use:

...a radiological bomb, in which conventional explosives disperse deadly radioactive poison, or

...even a nuclear weapon or bomb, perhaps concealed in any one of the more than 230 million cargo containers that move through the world's ports each year.

But there are other risks. This summary highlights the following threats, listed in order of their potential to wreak havoc on world trade:

CONCLUSIONS:

The Ultimate Doomsday Scenario

- 1) A nuclear weapon or bomb exploding in a port-city that is also a key node in the seaborne trading system and its land links to the global supply chain.

There are over 30 such mega-portcities spread over Asia, North America and Europe. They include:

In Asia - Hong Kong, Singapore, Shanghai and Yantian in China, Kaohsiung in Taiwan, Tokyo and Yokohama in Japan, Pusan in South Korea, and Laem Chabang in Thailand.

In the US - New York, Los Angeles, Long Beach, Charleston, Seattle, Norfolk, Houston, Oakland, Savannah and Miami.

In Canada - Vancouver, Montreal and Halifax.

In Europe - Antwerp in Belgium, Rotterdam in the Netherlands, Le Havre and Marseilles in France, London and Felixstowe in Britain, Bremerhaven and Hamburg in Germany, Genoa and La Spezia in Italy, Algeciras in Spain and Gothenburg in Sweden.

There is no evidence that Al-Qaeda or any other terrorist group has nuclear weapons. But they have shown interest in acquiring them. In the mid-1990s, Al-Qaeda agents tried repeatedly – though without success – to purchase bomb-grade highly enriched uranium in Africa, Europe and Russia. Two retired Pakistani nuclear scientists were detained in late 2001 after meeting Osama bin Laden in Afghanistan. They were later released without being charged, despite suspicions that the purpose of the meeting was to discuss how Al-Qaeda could make or acquire nuclear bombs. In November 2001, Osama bin Laden claimed that he had obtained a nuclear weapon, but US intelligence officials dismissed his assertion. Documents recovered from Afghanistan after the fall of the Taliban regime also described Al-Qaeda's nuclear ambitions. The CIA believes that bin Laden was seeking to acquire or develop a nuclear device.

However experts say that it would be difficult for terrorists to get enough plutonium or highly enriched uranium for a crude nuclear bomb and that even if they had the necessary fissile material, putting the infrastructure in place to build a usable bomb would probably take many years.

But experts note that building a crude, bulky, low-yield nuclear weapon, which could be smuggled to its target by ship, container or truck, would be far easier than making the compact, reliable, high-yield weapons found in US arsenals – and might well also be easier than stealing a nuclear warhead. Both warheads and fissile

material are closely guarded by the eight countries (nine if North Korea is included) known or thought to have them. The US, Russia and other countries are working with the International Atomic Energy Agency to secure bomb-grade material that could be stolen and sold to terrorists.

Still, the potential consequences of terrorists acquiring a nuclear explosive device could be so devastating and disruptive that it must be a matter of serious concern, even if the chances of it happening appear slim.

Nuclear weapons have been tested many times but only used twice. The two nuclear bombs dropped by the US on Hiroshima and Nagasaki in Japan in August 1945 to hasten the end of World War II were relatively small compared to many of the estimated 30,000 warheads in the arsenals of today's nuclear powers. But the Hiroshima and Nagasaki bombs destroyed both cities, turning them into mass graveyards poisoned by radioactive contamination.

The fissile core of the Hiroshima bomb was made of highly enriched uranium-235. It released a fireball of energy equivalent to 12.5 kilotons, or 125,000 tons, of TNT that caused severe burns and loss of eyesight. Thermal burns of bare skin occurred as far as 3.5 kilometers from ground zero, directly below the explosion point about 580 meters above central Hiroshima. Most people exposed to thermal rays within a one-kilometer radius of ground zero died. Tiles and glass melted in the intense heat. All combustible materials were consumed.

An atomic explosion causes an enormous shock wave followed instantaneously by a rapid expansion of air in an immensely powerful blast with typhonic winds. Concrete buildings near ground zero (thus hit by the blast from above) had ceilings crushed and windows and doors blown out. Many people were trapped under fallen structures and burned to death. Being anywhere within 500 meters of ground zero was fatal. People exposed at distances of 3 to 5 kilometers later showed symptoms of after-effects, including cancers induced by radiation.

The death count in Hiroshima in the wake of the atomic bombing is estimated to have reached 140,000 by the end of December, 1945. In Nagasaki, which was razed by a plutonium bomb, around 70,000 people were thought to have died by the end of 1945.

The Penultimate Doomsday Scenario

- 2) A radiological, or "dirty" bomb, exploding in a port-city that is also a key node in the seaborne trading system and its land links in the global supply chain.

A radiological, or so-called "dirty bomb" is a conventional explosive such as TNT or ammonium nitrate that has been packaged with radioactive material, which scatters when the bomb goes off. It kills or injures through the initial blast of the conventional explosive and by spreading life-threatening radiation particles; hence the term "dirty". A dirty bomb contains radioactive material, but does not use that material to produce a nuclear explosion.

Such a bomb may not be a real weapon of mass destruction, when compared to a nuclear explosion that could cause hundreds of thousands of deaths and injuries in a major city. But a radiological bomb would certainly be a weapon of mass disruption and panic if detonated in or near a city. Indeed, some US officials have said that dirty bombs, which could be constructed with relative ease by conventional bomb makers, may become the next weapons of choice for terrorists who want to cause panic and economic disruption.

The US government announced in June 2002 that it had arrested Jose Padilla, an American citizen and suspected Al-Qaeda operative, on his return to the US, thus disrupting “an unfolding terrorist plot to attack the United States by exploding a radioactive ‘dirty bomb’.” Padilla, a former Chicago gang member with a long and criminal record, had been in detention since May 2002 when he was taken into custody at Chicago O’Hare International Airport after arriving on a flight from Pakistan. He was carrying over \$US 10,000 in cash.

In August 2002, US prosecutors revealed further details in the case against Padilla in documents presented to a New York court. The prosecutors said that after his release from prison in the US in the early 1990s, Padilla traveled to Pakistan, Egypt, Saudi Arabia and Afghanistan, and became closely associated with the Al-Qaeda network, meeting with senior leaders of the group on several occasions while in Afghanistan and Pakistan in 2001 and 2002.

US officials said that Padilla had proposed the plan to build and detonate a radiological device, possibly in the US capital, Washington, to Abu Zubaydah, then Al-Qaeda’s top terrorism coordinator and a senior lieutenant of Osama bin Laden. Zubaydah was arrested in Pakistan in March 2002 and handed over to the US for interrogation.

Concerns about the risk of terrorists getting and using dirty bombs intensified in December 2003 when US prosecutors said that a British arms dealer, held in the US on charges of trying to sell shoulder-fired missiles to shoot down airliners, would face additional charges of plotting to procure a dirty bomb. Hemant Lakhani, 68, who was born in India but holds a British passport, was arrested in August 2003 in a sting operation involving intelligence agencies from the US, Britain and Russia. He was detained at a hotel near Newark International Airport and charged with trying to sell a missile imported from Russia to an FBI informant.

Depending on the sophistication and size of a dirty bomb, the radioactive material it dispersed, wind conditions, the location of the attack, and the speed with which the area was evacuated, the number of deaths and injuries from such an explosion might not be substantially greater than from a conventional bomb attack.

But panic over radioactivity and evacuation measures could snarl a city. Moreover, the area struck would be off-limits for at least several months during contamination clean-up efforts. This could paralyse a local economy and reinforce public fears about being near a radioactive zone.

The Federation of American Scientists told a Senate panel in March 2002 that radioactive materials that could easily have been lost or stolen from US research

institutions and commercial sites and incorporated in a dirty bomb could contaminate tens of city blocks at a level that would require prompt evacuation and create terror in large communities even if radiation casualties were low. Areas as large as tens of square miles could be contaminated at levels that exceed recommended civilian exposure limits. Since there are often no effective ways to decontaminate buildings that have been exposed at these levels, demolition may be the only practical solution. If such an event were to take place in a city like New York, it would result in losses of potentially trillions of dollars.

A radiological bomb attack could shut a port area for months for expensive decontamination. A severe attack could make large parts of a port-city uninhabitable for much longer.

Many counter-terrorism officials and analysts fear that a dirty bomb attack by terrorists, to carry their fight to a new threshold of horror, is inevitable. Eliza Manningham-Buller, the Director-General of MI5, Britain's domestic security service, said in June 2003 that it was only a matter of time before a terrorist attack using chemical, biological, radiological or nuclear technology was launched by Al-Qaeda or its affiliates against a big city in the West. "My conclusion, based on the intelligence we have uncovered, is that we are faced with the realistic possibility of some form of unconventional attack," she said.

The widespread availability of radiological bomb sources prompted scientists at the Los Alamos National Laboratory in the US to conclude, in a study released in September 2003, that a dirty bomb "attack somewhere in the world is overdue."

Radioactive materials are widely used and dispersed, not just for military purposes or for fuelling nuclear reactors to generate electricity. There are millions of other radioactive sources that have been distributed worldwide over the past 50 years, with hundreds of thousands currently being used, stored and produced for civilian purposes. The radiation from radioactive isotopes provides a low-cost way to disinfect food, sterilize medical equipment, treat certain kinds of cancer, find oil deep underground, check the welding in pipelines, monitor water aquifers, build sensitive smoke detectors and provide other important economic services.

As a result, radioactive materials are used in many thousands of hospital and medical centers, research laboratories, oil drilling facilities, food irradiation plants and other sites. Some are under government control; others in the hands of universities and the private sector. Many are not properly secured or accounted for. They have been lost, stolen or abandoned.

The International Atomic Energy Agency, the IAEA, has warned that the radioactive materials needed to build a dirty bomb can be found in almost any country in the world, and that more than 100 countries may have inadequate control and monitoring programs to prevent or even detect the theft of these materials. It has located at least 20,000 operators of significant radioactive sources worldwide. They include over 10,000 radiotherapy units for medical care, 12,000 radiography units, and about 300 irradiator facilities for industrial applications.

The IAEA is a United Nations agency that sets world standards for nuclear safety and security, and acts as a watchdog against diversion or illicit use of nuclear materials. Although 134 countries are members of the IAEA and can benefit from its assistance, over 50 countries are not.

The IAEA says that although radioactive sources may number in the millions, only a small percentage have enough strength to cause serious harm because they contain potentially lethal amounts of radioactivity. They include cobalt-60, strontium-90, caesium-137 and iridium-192 used in industrial radiography, radiotherapy, industrial irradiators and thermo-electric generators. These isotopes emit intense gamma rays that are useful in killing bacteria and cancer cells. The rays can penetrate clothing and skin to enter the human body.

Fortunately, building the most potent radiological bombs using these isotopes is much more difficult for terrorists than assembling explosives to disperse less toxic material. Not only are the very dangerous substances more difficult to obtain, the successful spreading of highly radioactive particles could only be done by a terrorist organization that had access to specialised scientific knowledge.

The Federation of American Scientists says that alpha particle emitters such as plutonium and americium could also be used in a dirty bomb to create a long-term health hazard and should be closely controlled as well. The alpha particles cannot penetrate clothing or skin but if inhaled can cause cancer. Plutonium, which is used in nuclear weapons, also has non-military functions. In the 1960s and 1970s, the US government encouraged the use of plutonium in university facilities studying nuclear engineering and nuclear physics. Americium is used in smoke detectors and devices that find oil sources.

Since 1993, the IAEA has compiled a list of at least 263 confirmed cases of trafficking or unauthorised movement of radioactive materials but admits that the actual number of cases is likely to be significantly larger, not least because only about 70 states are collecting and sharing information on such trafficking with the IAEA.

Of the cases brought to the IAEA's attention, the great majority appear to have been opportunists or unsophisticated criminals, motivated by hope of profit. But an important fraction of the cases involved persons who expected to find buyers interested in the radioactive contents of stolen sources and their ability to cause or threaten harm.

Criminals are now trading in components and materials for dirty bombs. Indeed, authorities report a dangerous surge of interest from this quarter that is complicating an already difficult task confronting governments: how to stop terrorists from acquiring powerful radiological sources.

No dirty bomb attacks have ever been recorded. But the BBC reported in January 2003 that British officials had presented it with evidence which they claimed showed that Al-Qaeda had been trying to assemble radioactive material to build a radiological bomb and may have succeeded in assembling a small dirty bomb in a nuclear laboratory in the Afghan city of Herat before US-led forces invaded Afghanistan in October 2001 to oust the Taliban regime that had allowed Al-Qaeda

and Osama bin Laden to train terrorists and organize international terrorist operations from Afghanistan. The alleged dirty bomb was never recovered.

But British officials said that Al-Qaeda certainly had the expertise to build another. They showed the BBC Al-Qaeda training manuals that set out details on how to use a dirty bomb to maximum effect.

Impact on Global Trade

The use of either a nuclear or radiological bomb in a major port-city would cut the arteries of commercial container cargo shipping if it was known or suspected that the device had been shipped in. It would bring much of the world's trade to a halt and severely damage the global economy, as governments in the affected country and those that did extensive seaborne trade with it scrambled to put in place extra security measures to protect their people, cities and economies.

Such measures would be drastic and include:

... lengthy cargo inspections in receiving as well as originating ports,

...or even the complete closure of ports for an indefinite period,

while additional checks and safeguards were put in place to allay public fears.

One of the first things the US government did after the terrorist attacks in September, 2001, was to shut US airspace and ground all civilian flights for four days – a security measure to protect the American public that had severe repercussions on aviation, travel, tourism and business around the world, including in Asia, as hundreds of scheduled flights had to be cancelled or diverted. The US government also closed US ports for two days.

Insurance

What would happen to insurance rates if terrorists attacked, or worse still closed, a major port, strait or waterway used for international trade? Ship and cargo insurance rates would skyrocket to prohibitive levels. The bigger the attack up the scale of terrorist violence, the greater the insurance shock would be.

There is no insurance for a maritime-related terrorist attack using a nuclear bomb. The recovery costs would be unimaginably huge. They would also be very heavy if a radiological bomb were detonated in a mega port-city. Whether private insurance payouts would be available to aid recovery from a dirty bomb explosion is doubtful.

Even a terrorist attack using a ship or ships to block one or more key international ports, straits or waterways – but not involving nuclear or radiological bombs – would trigger a damaging upward spiral in insurance rates and make many ships avoid the area. This is the third major risk for world trade from maritime-related terrorism.

Third-level Doomsday Scenario

3) A terrorist attack or a coordinated series of strikes that did not use nuclear or radiological bombs but instead used ships as weapons to close one or more key international ports, straits or waterways. The damage to world trade caused by such action would depend on how long the blockage lasted, the extent to which it could be bypassed and the costs involved.

Seventy five percent of global maritime trade passes through a handful of relatively narrow shipping lanes. Nearly 35 million barrels of oil per day – just under half the world’s daily consumption of nearly 78 million barrels in 2002 – passes through these same channels. Large amounts of another increasingly important source of commercial energy, natural gas in liquified form, or LNG, is carried through several of the same maritime arteries:

...Strait of Hormuz, the only sea entrance to the Persian Gulf. It is the gateway to the Arabian Sea and Indian Ocean;

...Malacca and Singapore Straits linking the Indian Ocean (and oil and gas supplies from the Middle East) with the Pacific Ocean (and major consuming markets in Asia) via the Andaman Sea and the South China Sea;

...Panama Canal connecting the Pacific and Atlantic Oceans;

...Suez Canal linking the Red Sea and the Mediterranean Sea;

...Bab el-Mandab passage from the Arabian Sea and the Gulf of Aden to the Red Sea;

...Bosporus and Turkish Straits, connecting the Black Sea and the Mediterranean.

These channels are critically important to world trade because so much of it passes through them. They are geographic “chokepoints” because they are narrow enough to be blocked, at least temporarily, by an accident or by an attack, including a terrorist operation. Many of the vessels that pass through these straits and canals are laden supertankers, or carriers of ammonium nitrate, liquified petroleum gas (LPG) liquified natural gas (LNG), chemicals and other inflammable, explosive or dangerous material that could be attractive to terrorists as floating bombs or major sources of pollution.

Of all the major international straits, the Malacca and Singapore Straits are the most vulnerable to attack and the easiest for a terrorist group to block, with the possible exception of the Bosporus and Turkish Straits. But the Malacca and Singapore Straits are far more vital to global seaborne trade than the straits that bisect Turkey. The closure of this key waterway in Southeast Asia would disrupt world commerce, although its impact would not be as catastrophic as a nuclear or radiological bomb attack on a mega port-city.

Over a quarter of world trade, half its oil pass and much of its liquified natural gas (LNG) pass through the Malacca and Singapore Straits between the islands of Indonesia to the south, and peninsular Malaysia and Singapore to the north. More than 80% of the oil imported by Japan, South Korea and China comes from the Persian Gulf via this waterway. Although over 600 miles long, the straits are congested and only 1.5 miles wide at their narrowest point in the Phillips channel near Singapore, the world's busiest port with a population of four million. As many as 50,000 large ships use the waterway each year.

The US Department of Energy has calculated that if the Malacca and Singapore Straits were closed, nearly half the world's fleet would have to sail further, generating a substantial rise in the requirement for vessel capacity, largely because of China's rapidly growing export-import trade. If this were to happen today, when demand for ships is exceeding supply, shipbuilding costs would rise.

Closure of the Malacca and Singapore Straits would also increase freight rates worldwide. It would jolt the economies of China, Japan, South Korea and Taiwan that rely on imported energy for continued growth. If the closure lasted for long, it could also be disastrous for Singapore's trade-dependent economy. Singapore is the 19th biggest trading nation and the 5th most trade-dependent country. The value of its trade is more than 80% of its GDP.

The Strait of Hormuz at the entrance to the Persian Gulf is just as important for world energy trade as the Malacca and Singapore Straits. Nearly half the world's oil and an increasing amount of its LNG flows through the Strait of Hormuz. But this strait is much less important for non-energy trade than the Malacca and Singapore Straits. It is also less vulnerable to closure than either the Malacca and Singapore Straits or the Bosphorus and Turkish Straits because it is a lot wider and more tightly guarded.

The Strait of Hormuz is some 40 nautical miles across, from Iran on one side and Oman on the other. Within the strait are separate 2-mile wide channels for inbound and outbound tanker traffic, with a 2-mile wide buffer zone between them. The Middle East, mainly the Persian Gulf, accounts for over 65% of the world's proven oil reserves and 36% of its proven gas reserves. Japan, South Korea and, increasingly, China are critically dependent on the Gulf energy supplies that pass through the Hormuz strait; the US and Western Europe are much less reliant on Gulf oil but still regard it as a key strategic chokepoint.

Closure of the Hormuz strait would have a huge economic impact on Northeast Asia and a major strategic impact on North America and Western Europe. This is why the US and its allies attach such importance to freedom of navigation through the strait, protect it with regular warship patrols, and station naval vessels in the Persian Gulf.

The Bosphorus and Turkish Straits are 17 miles long and barely half a mile wide at their narrowest point, much narrower than the Phillips Channel south of Singapore. The Turkish straits, which connect the Black Sea with the Mediterranean Sea, are the only southern shipping route for oil and commodities from Russia and the energy-rich Caspian Sea. The Black Sea is the largest outlet for Russian oil exports.

Two and a half million barrels a day of crude oil and refined products and 140 ships pass through the Bosphorus each day, or 50,000 vessels a year, the same number as use the Malacca and Singapore Straits. Of these, up to 8,000 carry oil or other potentially hazardous cargo.

Congestion is common, and the Bosphorus and Turkish Straits have often been closed following bad weather or accidents. Istanbul, a city of 10 million people, straddles the waterway. Citing safety concerns, Turkey has imposed restrictions on Bosphorus traffic. Two big truck bombs outside the British consulate and the British-based HSBC banking group killed more than 25 people in Istanbul in November, 2003, just five days after the bombing of two synagogues in the city left 25 dead. After these attacks, some analysts warned that the Bosphorus could be a tempting target for Al-Qaeda, although they saw no signs of a specific threat.

Terrorists Commandeering Ships

How could terrorists take control of a ship? They could collaborate with pirates or criminal gangs involved in the robbery or hijacking of vessels, especially in Southeast Asia where piracy is rife. In 2003, the International Maritime Bureau, an arm of the International Chamber of Commerce, named Indonesia's waters adjacent to the Malacca and Singapore Straits as the most dangerous on the planet, accounting for 87 of the world's 344 pirate attacks in the first nine months of the year.

But it is more likely that Al-Qaida would use its own ships, or its own agents to take control of a vessel, for a major maritime terrorist attack. This would give the organisation better control over any operation. Otherwise it would have to rely on people from outside its circle of zealots, whom it might not be able to trust. Moreover, for pirates, and any criminal syndicates behind them, a serious terrorist attack would be bad for business-as-usual because it would almost certainly lead to a crackdown that would make future sea robberies more difficult.

RECOMMENDATIONS:

A) Disaster Prevention -

... TIGHTER SECURITY OVER NUCLEAR WEAPONS, FISSIONABLE MATERIAL, RADIOACTIVE SUBSTANCES, EQUIPMENT AND TECHNOLOGY THAT COULD BE ACQUIRED BY TERRORISTS AND USED TO MAKE NUCLEAR OR RADIOLOGICAL BOMBS.

The US and other governments have established programs to keep fissionable materials for making nuclear bombs out of terrorists' hands. Since 1994, the US has spent several billion dollars in collaboration with Russia to secure nuclear weapons and materials in the former Soviet Union and Yugoslavia and to provide alternative jobs to some of the more than 10,000 former Soviet weapons designers, nuclear scientists and energy experts who were employed during the Cold War.

But in October 2003 a report co-sponsored by the US-based Nuclear Threat Initiative, an anti-proliferation watchdog headed by former US Senator and arms control expert Sam Nunn, said that only a tiny fraction of a total \$US 20 billion

pledged by the Group of Eight leading powers in 2002 to secure global stockpiles of nuclear, chemical and biological materials had been spent or even allocated to specific projects. In 2002, less than half Russia's fissile material was judged to be secured.

Nunn said that the war in Iraq had distracted the US and diverted resources away from the need to secure weapons of mass destruction in regions such as the former Soviet Union. The report pointed out that there are some 100 poorly protected research reactors, spread across 40 countries, containing weapons-usable uranium and that to construct a nuclear bomb, terrorists would need to steal only a small amount of nuclear material, about enough to fit in a suitcase. "The threat is outpacing the response," Nunn said.

Clearly, more needs to be done by the nuclear powers, in collaboration with the International Atomic Energy Agency, the IAEA, to secure fissile material and nuclear weapons. Just as urgent, although less well known, is the threat from other radioactive materials that could easily find their way into the hands of terrorists.

As already noted in this report summary, the IAEA, has warned that the radioactive materials needed to build a dirty bomb can be found in almost any country in the world, and that more than 100 countries may have inadequate control and monitoring programs to prevent or even detect the theft of these materials.

This is an open invitation for terrorists and traffickers to move in and get the materials to make radiological bombs. Indeed, there is evidence that they are seeking to do this. The IAEA needs more support from UN member states, more money and more resources to do its job effectively and prevent a dirty bomb being made and used.

...A UNIVERSAL CONTAINER INITIATIVE IS NEEDED TO SUPPLEMENT THE US-DRIVEN CONTAINER SECURITY INITIATIVE AND PROVIDE BETTER SECURITY THROUGHOUT THE GLOBAL SUPPLY CHAIN TO PREVENT A NUCLEAR OR RADIOLOGICAL BOMB BEING PLACED IN A CONTAINER OR ON A SHIP INVOLVED IN INTERNATIONAL TRADE.

A container checking system similar to the CSI needs to be adopted by all ports for all destinations that are significant links in the seaborne supply chain powering the world economy. Both the US and the EU appear to recognise the importance of expanding the coverage of the CSI. At present, only containers bound for the US are being checked, although Canada and Japan have accepted a US offer to screen any suspect containers in American ports before they leave for Canada or Japan.

The US and the EU agreed in November 2003 to work out ways of ensuring the security of containers from all locations that are imported into, transhipped through, or transit the EU and the US. This would amount to a very large portion of the world's general cargo trade. Leading Asian traders should adopt a similar approach. This would be the genesis of a Universal Container Initiative.

The International Maritime Organisation and the World Customs Organisation are the most appropriate multilateral forums for coordinating such a strategy. The

Organisation for Economic Cooperation and Development, the OECD, based in Paris is studying how to ensure the integrity of seaborne containerised cargo throughout its journey, from the point on land where it is loaded and sealed in the container to the point where it is unloaded for delivery after the ocean voyage.

...HARNESS TECHNOLOGY AND TAP THE PRIVATE SECTOR

It should be possible to implement a more universal system of container security over the next few years as new technology for 'smart and secure' containers becomes widely available and costs come down. These IT-enabled containers will have satellite-communication connections so that they can be tracked remotely at all times when loaded. They will have electronic seals, as well as physical locking systems, to prevent unauthorised opening. They will also contain sensors to detect explosive, radioactive, and harmful chemical or biological substances. Non-invasive scanners using X-ray, Gamma-ray and other technologies will also improve.

Companies owning containers could be encouraged by tax incentives as well as government regulation to introduce the 'smart and secure' containers.

...SECURITY MUST TAKE PRIORITY OVER SECRECY IN SHIPPING

Lifting the shroud of secrecy covering the ownership and control of ships, and improving seafarer recruitment and identification, are critically important in preventing terrorists from using ships for their own purposes. Failure to do so will mean that terrorists can work within, and under the cover of, the new maritime security arrangements that have already been applied or will be in place by the end of 2004.

Seafarers are to be issued biometric identification documents by their governments to guard against terrorist infiltration. To reinforce this, the International Maritime Organisation should develop a database of all seafarer certificates and work with its member-states to crack down on fake papers.

To guard against a serious terrorist crime involving a ship, law enforcement authorities may need to find out who actually owns the vessel and controls its movements and operations. Real, or beneficial, ownership is not only disguised by the widespread practice of putting ships on foreign registers. The long-established tradition of having companies, not individuals, own ships also makes checking ownership, for security reasons, difficult. The practice can be justified in commercial terms: individuals naturally want to avoid personal liability for any accidents their ships may have. But the practice of making the registered owner or owners of a ship no more than a "brass plate" corporation provides an almost impenetrable cloak of anonymity.

Open, or flag-of-convenience, registers – which by definition do not have any nationality requirements – are the easiest places in which to register vessels that are covered by complex legal and corporate arrangements. But it is not so much the registers themselves that enable reclusive owners to hide their identities. It is the corporate arrangements that are widely and legally available in many countries to shroud the ultimate owners in anonymity, even if they are terrorists.

The OECD Maritime Transport Committee is studying the various ways in which a cloak of secrecy can be created around the ownership of vessels. It will then identify best practices that would enhance transparency without breaching the confidentiality of commercially sensitive, but non-security-related, information.

Most open registers do not require audited accounts from the shipping companies that use them, including some of the largest registers, among them Panama, Liberia, Bahamas and Belize. A number do not reveal the names of shareholders or directors, as in Liberia, Bahamas and Belize. It is easy and inexpensive for an owner to hide behind a string of companies. Bearer shares – which, as the phrase suggests, can be passed from one individual to another and carry ownership rights – are allowed in many of the countries that offer open registers. Secrecy in the name of business confidentiality is the norm in the flag of convenience system.

The US argues that even though its domestic laws permit “brass plate” corporations to own ships, the use of this device to hide the identity of terrorist organisations that threaten the safety and security of ships, ports and people cannot be justified on any basis. In the US itself, the US government has the authority to require detailed ownership information through all corporate layers to ensure that vessels registered in the US comply with US documentation laws. The aim is to find out who actually controls the movements or operations of the ship, or who derives profits from its trade.

The US insists that a flag state must provide a port state (meaning the country where the vessel is calling) accurate and complete ownership information for maritime security purposes if requested. Washington has proposed that the International Maritime Organisation develop international standards so that, in cases where there are reasonable grounds for suspecting terrorist connections, the identify of the person or entity in actual control of the vessel can be speedily made known to authorised security personnel. It suggests that such standards should make clear that the person providing the information, i.e., the captain of the vessel, the agent or owner, must provide a complete and accurate account, and that the port state will continue to apply domestic law in its internal waters in cases of false reporting, meaning that sanctions or legal penalties can be imposed.

The US acknowledges that complex issues are involved. But it says that there is precedent for flexible interpretation of ownership and control in the international Customs Convention on Containers of 1972, a mode of shipping that has also raised significant maritime security concerns. This convention avoids defining the “owner” of a container. Instead, it places the onus for ensuring security on the operator – the person who, whether or not the owner of the container, has effective control of its use.

...THE ULTIMATE SANCTION IS PORT STATE CONTROL AND IT SHOULD BE STRONGLY ASSERTED TO MAKE ALL SHIPS, PORTS AND COMPANIES COMPLY WITH THE NEW MARITIME SECURITY STANDARDS MANDATED BY THE IMO.

Many countries and companies, particularly the smaller and less affluent, complain of the difficulty and costs in meeting the new security standards. In some cases, financial aid and technical assistance may be warranted to make compliance possible for governments and ports in developing countries. Industrialised nations, and regional agencies such as APEC, the Asia Pacific Economic Cooperation forum, and the Asian Development Bank, are already helping governments and ports in developing countries to raise their security levels to meet international standards and join the US-sponsored Container Security Initiative. More help may be needed on the basis that security is only as strong as the weakest link in the chain.

But the International Maritime Organisation should not extend its deadline for implementing its new standards, which in most cases must happen by 1 July 2004. Too much is at stake for world trade and global security for slippage to be tolerated. The fact is that most countries, ports and shipping lines with a major interest in seaborne commerce will comply, if they have not already done so, because the costs of non-compliance far outweigh the costs of conforming.

Until quite recently, port state concerns – even in countries like the US which face an acute terrorist threat – have focused on safety, rather than security. The new security measures, combined with an assertion of port state control, will put enormous pressure on all ships and ports that are involved in international trade to conform with the standards set by the IMO and powerful trading nations or blocs such as the US and the European Union.

The IMO has told shipowners that they must implement its security measures in 2004 or face severe restrictions on their movements. Tankers, cargo ships, cruise liners and other large vessels travelling to foreign destinations must obtain the IMO's International Ship and Port Facility Security certificate by 1 July or they will no longer be admitted into foreign ports.

Ships that don't pass the security tests will be liable to fines or exclusion. This will force sub-standard vessels to improve or become pariahs of the sea. Failure by a port to comply with the security standards by 1 July 2004 will allow other countries to delay or bar vessels which visited that port.

B) Disaster Recovery -

...SET UP AN INTERNATIONAL SYSTEM FOR DEFUSING A MASS TERROR BOMB OR COPING WITH THE AFTERMATH OF AN EXPLOSION.

Many countries have drawn up plans for managing a major terrorist attack on their ports and cities, although how effective they would be in coping with the mass panic following a radiological bombing or the horrific devastation and casualties after a nuclear explosion is open to question because they have never been activated to deal with such catastrophes.

Industrialised nations and some other countries have emergency response units and procedures in place to defuse a radiological or nuclear bomb found in their national jurisdiction before it explodes.

Given the impossibility of completely securing seaborne trade and the global container cargo supply chain, and given the growing risk that terrorists will resort to mass violence, possibly by using a dirty bomb on a ship or in a container, in or near a key port-city or international shipping strait, the five declared nuclear powers, (the US, Britain, France, Russia and China), or as many of them as are prepared to act, should establish a mechanism for coordinating the prompt despatch of technical teams to help any country threatened by a terrorist weapon of mass destruction or a radiological bomb to neutralise it.

Since speedy action would be vital, three other known nuclear powers – India, Pakistan and Israel – should also be called upon to assist if necessary, based on their geographical proximity to the crisis point. The country in which a wmd or dirty bomb was found would need to request outside help if it was unable cope by itself. Such an assistance mechanism could be linked to the International Atomic Energy Agency, the United Nations body responsible for nuclear and radiological safety. If a wmd or dirty bomb exploded, the same channel through the IAEA could be used to coordinate the international assistance required to cope with the disaster and recover from it.

America has a special responsibility in this regard, since it has insisted that all containers arriving by sea in its huge market – the world’s largest - be checked for wmd and dirty bomb materials in foreign ports. The US, which has a large reservoir of expertise and technical know-how to disarm nuclear and radiological bombs, calls the CSI a defence-in-depth strategy. In effect, however, it is foisting on other countries the potentially terrible consequences of mass terror aimed primarily at America.

Many of those countries do not have the resources and capacity of the US to defuse nuclear or radiological bombs or cope with the devastating aftermath if they explode. US policy on the CSI is an application of the NIMBI (Not-In-My-Backyard) syndrome. It is perfectly understandable in the climate of terrorist threat that surrounds the US. But it will be seen, rightly, by many other countries as a policy of utter selfishness that is being enforced by the world’s sole superpower unless it is accompanied by a readiness to help cope with the possible consequences.

...THE MARITIME SUPPLY CHAIN NEEDS A “RESTART” MECHANISM IN CASE IT IS HIT BY AN ACT OF CATASTROPHIC TERRORISM.

This report concludes that if a nuclear or radiological bomb was brought by sea into a major port-city or international shipping strait and exploded, it would halt or severely disrupt world trade. The global seaborne supply chain can probably never be made immune from this kind of attack. The fight against terrorism is likely to last for years. A key issue facing policy planners must therefore be how to build a global seaborne supply chain that is sufficiently resilient to withstand a devastating shock and resume operations quickly enough to avoid precipitating a world economic crisis.

How long would it take for port and shipping trade to get up and running again if a terrorist catastrophe happened? There are at present no agreed international arrangements for reviving the maritime supply chain system after a crisis; there is no “restart” button or mechanism. This is serious gap that needs to be filled. One way of

doing so may be to add a security mandate to the work of the World Trade Organisation, much in the way that APEC, the Asia Pacific Economic Cooperation forum, has been given responsibility for promoting and facilitating secure trade in the APEC region.

The author – Michael Richardson, a former Asia Editor of the International Herald Tribune, is a Visiting Senior Research Fellow at the Institute of Southeast Asian Studies. His current research focuses on maritime, energy and sealane security. The views expressed, and the recommendations made, in this report are those of the author. He welcomes comments on the report.

Address: 5 Pasir Panjang Rd #07-29, Singapore 118494.

Telephone: 65-64791356

Email: mriht@pacific.net.sg