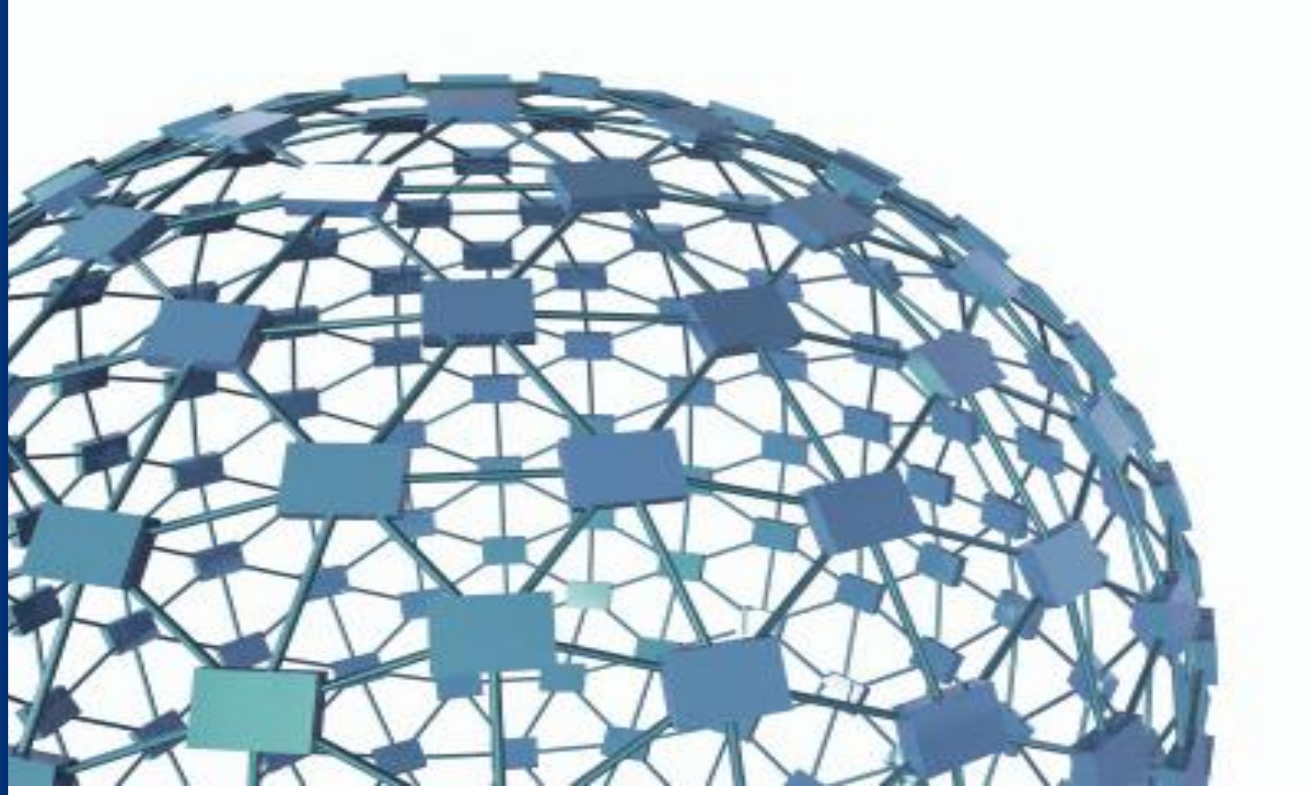
ILLICIT TRAFFICKING CHALLENGES

FIGHTING THE GOOD FIGHT AGAINST ILLICIT TRAFFICKING NETWORKS



JAMES A. RUSSELL
Naval Postgraduate School

and

JACK BOURESTON
FirstWatch International

OCTOBER 2012

U.S. NAVAL POSTGRADUATE SCHOOL • CENTER ON CONTEMPORARY CONFLICT

PASCC REPORT NUMBER 2012 012

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Illicit Trafficking Challenges: Fighting the Good Fight Against Illicit Trafficking Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School (NPS),Center on Contemporary Conflict (CCC),1411 Cunningham Road,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**32**	

ILLICIT TRAFFICKING CHALLENGES

FIGHTING THE GOOD FIGHT AGAINST ILLICIT TRAFFICKING NETWORKS

James A. Russell
Naval Postgraduate School (NPS)

and

Jack Boureston
FirstWatch International

October 2012

This report is the product of a collaboration between the Naval Postgraduate School, Center on Contemporary Conflict, and the Defense Threat Reduction Agency.

The views expressed herein are those of the authors and do not necessarily reflect the official policy or position of the Naval Postgraduate School, the Defense Threat Reduction Agency, the Department of Defense, or the United States Government.

U.S. Naval Postgraduate School (NPS),
Center on Contemporary Conflict (CCC)
Project on Advanced Systems and Concepts for Countering WMD (PASCC)

Project Cost: $168,846

Report Number 2012 012

The Naval Postgraduate School Center on Contemporary Conflict is the research wing of the Department of National Security Affairs (NSA) and specializes in the study of international relations, security policy, and regional studies. One of the CCC's programs is the Project on Advanced Systems and Concepts for Countering WMD (PASCC). PASCC operates as a program planning and implementation office, research center, and intellectual clearinghouse for the execution of analysis and future-oriented studies and dialogues for the Defense Threat Reduction Agency.

For further information, please contact:

The Center on Contemporary Conflict

Naval Postgraduate School

1411 Cunningham Road

Monterey, CA 93943

ccc@nps.edu

or

OSRDInfo@dtra.mil

CONTENTS

INTRODUCTION

Events such as September 11, 2001, and the revelation that the Khan Nuclear Network helped known proliferators obtain needed equipment prompted international focus on illicit procurement networks. This study focuses on those efforts, considers their effectiveness, and asks what more can be done.

METHODOLOGY

The study was commissioned by the Defense Threat Reduction Agency. It is the fourth in a succession of investigations, conducted by James Russell and Jack Boureston into the workings of illicit procurement networks and the efforts that the international community is taking to stop these networks.

Russell and Boureston set out to answer the following questions: Are there any practices that procurement agents use to elude law enforcement authorities? Why does the illicit trade of sensitive technologies continue? Why haven't individual nations and the international community been able to stop illicit traffickers? What more can be done to stop illicit procurement networks?

To answer these questions, the investigators reviewed secondary sources since 2009 (the end of their third investigation of networks) and contacted a number of international experts who have focused on illicit trade issues to get their perspective on the problem and possible solutions.

KNOWN FACTS ABOUT ILLICIT PROCUREMENT

Since the beginning of the industrial revolution, states have looked externally to supplement their knowledge of new technologies and to obtain needed materials. In cases where nations have built weapons of mass destruction (WMD) – chemical, biological, radiological and nuclear (CBRN) weapons – their success was based on the acquisition of vital equipment, materials, and know-how from foreign entities. History has recorded time and time again examples of nations sending agents to far off lands to acquire designs and recruit technicians in support of indigenous efforts to develop WMD systems.[1]

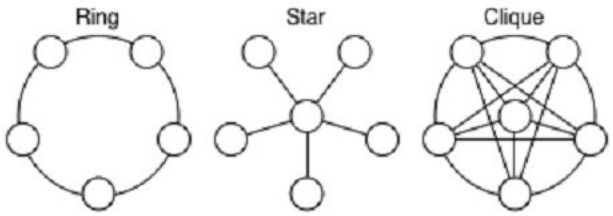
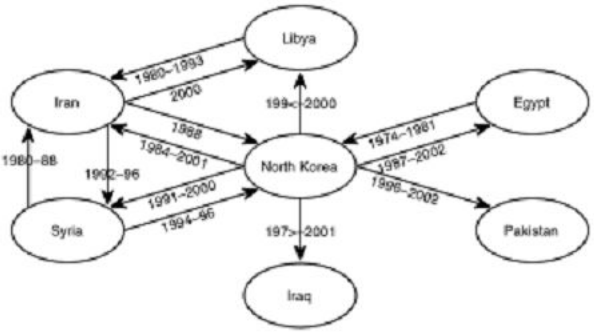
Despite new international efforts to stop the spread of sensitive technologies, illicit procurement activities continue.[2] In January 2012, the U.S. Department of Justice (DOJ) reported on more than 250 cases over a 5-year period of nationals from China, Colombia, Iran, Nigeria, Pakistan, Syria, Venezuela, and other countries conspiring to procure various high tech items that could be used to further their country's military programs.[3] The DOJ only records

U.S. cases, but similar numbers might be found in other industrialized countries such as Japan, the United Kingdom, France, Germany, and Canada.[4] And these are only the known cases. There must be a number of cases that are unknown and successful. States and non-state actors continue to inch closer to developing weapons that one day will threaten peace and stability in the world.

Network Structures

What do networks look like? In his 2005 *International Security* article, "Ringing in Proliferation," Alexander Montgomery describes three basic illicit procurement network structures: Rings or Circles; Stars; and Cliques. According to Montgomery, **Rings** are created with connections between nodes to form a circle; **Stars** are fashioned with nodes connecting through a central hub; and in **Cliques** nodes are connected to each other directly to form a network.[5] Most nuclear procurement networks appear to be Star structured, with a central hub providing direction and nodes operating semi-autonomously. However, North Korea and other countries may have created Clique structured networks with nodes that help other nodes acquire needed technologies and share it among them all. Through his analysis, Montgomery was able to map interactions between North Korea, Iran, Pakistan, and possibly others.[6]

Figure 1. Network Structures

Simple Network Structures	Missile Network Structure
	

Source: Montgomery, "Ringing in Proliferation," *International Security*, Fall 2005.

Changing Structures?

In her paper "The New Face of Illicit Trafficking Networks," Ashley Nilsen asserted that, networks no longer follow a traditional, hierarchical model of operations, but instead have transformed into a "network of networks," that is loosely connected with a common purpose, but operates independently with no responsibility to a central organization.[7] This may define the Khan network better than any other depiction. Although it began as a network to support

Pakistan's nuclear program, it became a loosely formed conglomerate that operated independently to support the demand of Khan's clients; Iran, Libya and North Korea.

Case Studies

This section describes examples of state illicit procurement activities to acquire WMD-related technologies.

Pakistan

In 1974, in response to India's peaceful nuclear explosion (PNE), the Pakistani government organized a clandestine group under the Pakistan Atomic Energy Commission (PAEC) to build a nuclear weapon. Recognizing that it lacked various equipment and technologies, the PAEC established a multi-layered procurement group to seek technologies around the world, while evading international detection and controls. This group enlisted nationals that were living abroad to approach local suppliers; made purchases and shipping materials to Pakistan**;** acquired piece parts rather than whole assemblies; mislabeled critical components on long lists of useless materials; paid exaggerated prices to entice suppliers to overlook export license requirements; requested samples that could be re-engineered; purchased raw materials and the machines needed to manufacture components and produce complete assemblies; established transshipment routes; and cooperated with friendly countries such as China, Libya, and North Korea to obtain needed materials**.**[8] During the 1970s and 80s, Pakistan's purchasing agents visited companies and met with representatives to attain needed goods, services, and knowledge. The agents courted organizations that were sympathetic to Pakistan's quest to gain parity with India or were just willing to sell goods at a marked-up price.

In what is now the most publicized case on nuclear networks, A.Q. Khan, a Pakistani national who worked in the Netherlands in the early 1970s, helped his country establish a procurement network. Not only was Khan instrumental in supporting Pakistan's program, he also assisted programs in Iran, Libya, and North Korea. According to Mark Hibbs at the Carnegie Endowment for International Peace, "It is important to underscore that, unlike cases in which national governments tightly managed clandestine procurement activities to develop nuclear weapons, the activities of the Khan network were apparently not steered by a national government but were carried out in parallel with Pakistan's nuclear weapons program and involved scores of non-state actors – engineers, manufacturing companies, traders, brokers, and financiers – none of whom were acting on behalf of any national government authority."[9]

Khan's procurement network used intermediaries in Austria, Dubai, Germany, Japan, Malaysia, the Netherlands, Singapore, South Africa, Switzerland, Turkey, the U.S, the UK, and other countries. The network was made up of Khan's former school mates, colleagues, and contacts. Its loose connections underscore the importance of social networks as a basis for developing and operating any business. Khan used his network to seek out and acquire needed items. He established transshipping points in Turkey and Dubai while manufacturing operations were located in South Africa and Malaysia. Khan also trained his clients to use the machining tools that he purchased for them, so they could manufacture needed equipment for their programs.[10]

Although it was a vast and loosely linked network, Khan maintained some form of control over its activities. According to Bruno Gruselle, a prominent French expert on illicit procurement networks, "The A.Q. Khan Company appears to have always operated on the principle of a direct initial contact between the network leader and his customers. Once contacts had been made and main principles had been defined, Khan appears to have left his main associates responsible for operational implementation."[11] Although initially working for his country only, Khan at some point must have realized that he could profit from the interest of other countries' intent on developing an indigenous nuclear program. By this time, Khan operated totally outside of his government's controls. He extended his network to not only include Pakistani nationals living overseas, but also foreign friends and colleague. Khan also encouraged his associates to enlist family members and friends to assist in the network's operations.

There is evidence that Pakistan continues to operate a network of buyers that includes nationals living around the world. The network continues to contact suppliers and purchases sensitive materials for shipment back to Pakistan. A recent example is the case of Nadeem Akhtar, a Pakistan citizen, who between 2005 and 2010 worked with Pakistani associates living in the U.S. to acquire equipment such as valves, switching equipment, coolant water purification devices, and calibration equipment. The group evaded export restrictions by undervaluing and falsely describing items being exported; hiding the true end-user of the equipment by using third parties and/or faking business entities in locations such as Dubai and the United States; using other individuals in Illinois and California to procure items for them under false pretenses; shipping items to his residences in Maryland so it would appear as though Akhtar's company was the end-user; and transshipping the equipment from the U.S.

through the United Arab Emirates (UAE). Akhtar took his direction from a trading company in Pakistan that was filling orders from the Pakistani government.[12]

Iraq

In the early 1980s, Iraq created a sophisticated procurement network similar to that of Pakistan's to help it obtain equipment for its WMD programs. The Ministry of Industry and Military Industrialization (MIMI) coordinated Iraq's commercial, diplomatic and intelligence entities, and established front companies to make inquiries for procuring items. Iraq's agents also mimicked many of the techniques developed by Pakistan to evade the export controls of other nations.

Iraq used its embassy personnel to help it identify willing sellers of equipment needed for its program. In one case, in the early 1980s, Ali Abdul Muttalib, commercial attaché at the Iraqi embassy in Bonn, Germany identified companies that could fill item requests, and learned how to elude European export controls by describing equipment in a way that would hide their true utility.[13] Muttalib set-up buying missions for Iraqi delegations and put them in touch with local company representatives. In 1987, he organized a visit of Iraqis to Germany to purchase goods such as HEU processing equipment and high speed measuring devices to help Iraq develop high explosive lenses for nuclear weapons. Muttalib introduced his Iraqi colleagues to Werner Sonntag, a representative of the engineering firm Neuero and import/export company Inwako. The Iraqis gave Sonntag a long list of explosive test equipment and the technologies that they needed and Sonntag found it for them. He also found and provided other equipment such as ring magnets to stabilize centrifuges, and rotor stand equipment to stabilize Iraq's missile systems.[14]

Iraq frequently used outside experts in countries such as Germany to obtain needed materials for their nuclear program. In the mid-1980s, Bruno Stemmler, a former MAN Technology employee who had dealings with the Iraqis, introduced Karl Heinz Schaab, also a former MAN Technology employee, to his Iraqi contacts for possible work. MAN was a principal at a company who contracted to the URENCO uranium enrichment consortium for services. Schaab helped Iraq acquire URENCO centrifuge rotors and the machine tools necessary to manufacture them. Iraqi agents often found companies such as Schaab's that were small and needed infusions of capital.[15] Schaab and his colleagues made at least two shipments to Iraq. The first was a box of rotor samples, sent in 1989. The next year, Schaab manufactured 20 complete rotors and shipped them to his Iraqi buyers via an Austrian transshipper.[16]

As a part of its network, MIMI established a series of front companies to procure items. MIMI used practices such as disguising shipment's final destination and misrepresenting the end-use of material to elude controls. For example, in the 1980s, MIMI set-up the Al-Arabi Trading Company and Nassr General Establishment to procure materials for Iraq's unconventional weapons programs. Iraq used these companies to purchase controlling stocks in other companies to obtain needed items. For instance, in 1987, Al-Arabi secretly purchased a 50 percent stake of the German Firm H & H Metalform GmbH, which provided the Iraqis with flow-forming machines and specialty parts for missiles.

Some front companies installed subsidiaries in neighboring countries such as Jordan to facilitate the procurement and shipment of goods into Iraq. In the early 1990s, the Sattam Hamid Farhan al-Gaaod Company established the Al-Eman Commercial Investment Group to organize material flows through Jordan to Iraq. The group regularly mislabeled the contents of packages and disguised end-users to quell suspicions of illegal activities. Within the Iraq Survey Group's final report, the Al-Eman Commercial Investment Group was noted as a large group of front companies with subsidiaries operating in Baghdad, Dubai, and Amman.[17] Throughout the 1990s, Al-Eman shipped at least one container a month through Jordan to Iraq via the Iraqi Embassy in Jordan.[18]

North Korea

In the course of its development of weapons of mass destruction, North Korea has emulated the illicit procurement practices of Pakistan, Iraq, and Iran. These practices include using nationals living abroad to help identify, acquire, and ship needed equipment home, operating front companies to purchase and ship material, and using third party suppliers and intermediaries to acquire materials and know-how.

In 1946, North Korean nationals living in Japan created the Association of the Scientists of North Korean Residents in Japan. Shortly thereafter, the Association created the Korean Association of Science and Technology (KAST), which has been an effective conduit for illicit procurement of material and access to know-how from Japan into North Korea. KAST is under the direct control of the external relations division of the Korean Workers Party (KWP) in Pyongyang. It is comprised of approximately 1,200 members, some of which work in fields such as physics and engineering.[19] The group operates 12 branches all over Japan. Its members work in research institutes, national universities, and technology companies. Some of these organizations have been implicated in the transfer of materials to North Korea.[20] In 1993, Daiei – a KAST affiliated company – arranged for the export of measurement equipment to North

Korea. In 1994, Japanese authorities discovered that another KAST related company had transferred a jet mill machine – equipment used to grind materials finely – to North Korea.[21]

Since the 1950s, North Korea has looked to South Korea as a portal for obtaining needed goods and knowledge that is required for its industrial development. For decades, the two Koreas have held scientific and educational exchanges to foster better relationships between the two countries. These exchanges have also facilitated transfers of goods and assistance to the North. In one case in 2004, four employees of Japan's Horkos Corporation attempted to send five-axis machining tools to South Korea and ultimately to North Korea. In an effort to evade Japan's Ministry of Economy, Trade and Industry (METI) licensing requirements, the employees mislabeled the items and declared on export declarations that the tools did not require export licenses. Although these tools can be used to manufacture automotive components and other commercial items, they are also used to produce uranium centrifuge components.[22] Investigators believe that the employees sent more than 1,000 of the five-axis machine tools to 16 countries by falsifying export documents in this way.[23]

In the 1970s, North Korea began deploying agents around the world to contact nationals living abroad and acquiring items that were needed to support the North's WMD programs. North Korea's procurement agents used A.Q. Khan's list of nuclear suppliers to identify needed equipment and acquire it. To help with these activities, the North created Office 39 in the Portuguese colony of Macao. The Office became a key offshore center for North Korean procurement. It ran a number of front companies such as the Zokwang Trading Company and the Daesung Chongguk Company, which had offices in Austria to reach out to European suppliers, purchase equipment, and ship it to North Korea. These companies used Macao's lax banking policies to pay for goods and move money back to their home country.[24] In 2002, North Korean experts attempted to procure 22mt of 6061-T6-grade aluminum pipes from Optonic GmbH in Germany[25] and imported 2600 aluminum tubes from Russia.[26] In addition to targeting European companies for materials, North Korean diplomats recruited South Korean intellectuals living in Germany help purchase materials.[27]

The North operated (and may still operate) a logistic system between itself and Japan to transport items home without raising suspicions. Specifically, the North Korean ferry *Man Gyong Bong* that runs between the North and Japan was used to ship items home. According to news reports, before the Taepo-Dong-1's first test launch in 1997, missile components were regularly exported from Japan to North Korea.[28] In 2003, the Tokyo Vacuum Corporation, a vacuum pump maker, and an export agent Nakano Corp conspired to transport vacuum

pump(s) useful for uranium enrichment to North Korea via a Taipei Taiwan company.[29] And between August 2006 and August 2007 another Taipei company HuaYueh International, made as many as 14 shipments of Japan origin dual-use items (including stainless steel pipes, computer software and computer numerical controlled machine tools) to North Korea. The company reportedly labeled the point of destination as China.[30]

In 2009, Japanese police arrested officials at the trading firm, Tokyo Boeki for the attempted export of a magnetometer (a device used to measure magnetic fields and useful in the development of missile guidance systems) to Myanmar.[31] The company was filling an order made by the Hong Kong based front company New East International Company.[32] Tokyo Boeki apparently exported a number of dual use items to Myanmar that eventually made their way to North Korea. The items included a cylindrical grinder used to produce magnets used in missile components and in uranium centrifuges.[33] In a Center for Nonproliferation Studies report, Robert Shaw and his colleagues posited that "Myanmar has distinct advantages to North Korean procurement networks that want to circumvent sanctions and illegally-divert dual use equipment to Pyongyang. Although it is subject to sanctions, Myanmar is not as isolated as North Korea, and legitimate shipments originating from Japan, for example, provide suitable cover for WMD-related deliveries."[34]

Iran

Since the 1970s, Iran has acquired nuclear-related material and equipment, designs, and know-how from countries such as China, France, Germany, Japan, the Netherlands, Pakistan, Russia, Switzerland, and the United States. Iran's system of procurement appears to be modeled after Pakistan's. Persons working in Iran's embassies contacted companies and individuals located in industrialized countries to acquire related material and ship it back to Iran. Sometimes they established front organizations to falsify supplier nation's end-user certification requirements. Iran's use of universities as fronts is well documented. Of the many universities that are a part of Iran's procurement network, Sharif University of Technology is key. In 1991, entities at Sharif purchased ring magnets from the German firm Thyssen.[35] Another German company, Karl Schenck of Darmstadt (now simply Schenck), sent at least one balancing machine to the university. The machines are used to balance equipment such as turbines, pumps, and compressors. They are also used to balance uranium centrifuges. In 1993, the Swiss firms AGIE and Charmilles transferred electrical discharge machinery (EDMs) to Sharif. EDM is a key to manufacturing molds and tools for the mass production of plastic and metal arts, and useful in the machining of complex precision parts such as centrifuge components.[36]

Iran is known to use nationals living abroad to procure needed material. The following are some examples. In 2002, Eddie Johansson, a 37-year-old Swede of Iranian origin, allegedly arranged for the purchase of 44 high-voltage switches from the German company Behlke Electronic GmbH. Johansson's brother, Abdollah Nagash Souratgar,[37] reportedly sent German mechanical engineer Harold Hemming a bank transfer of $72,337.80 for the purchase of the switches. Hemming asked his friend Eva-Marie Hack to place the order for the switches under the name of her company, CTC Offices Services. According to investigators, the company was phony, lacking any staff or assets.[38] Between 2002 and 2005, Mohammad Reza Vaghari and Mir Hossein Ghaemi used their Saamen Company in Pennsylvania, U.S.A., as cover to purchase a number of laboratory instruments then send them to Iran via the United Arab Emirates (UAE).[39] Between 2007 and 2008, Jirair Avanessian, an Iranian living in California, and his associates appear to have made more than seven shipments of vacuum pumps with uranium enrichment applications to Iran. He re-labeled and undervalued the contents of each shipment to mask the true value of the contents and avoid interception by U.S. Officials. In most cases, Avanessian prepared airway bills that mislabeled the contents as spare parts to avoid having to make export declarations.[40] He directed the supplier to ship the equipment to a company in a UAE free trade zone, thus making it appear that the UAE company was the ultimate destination. Avanessian directed the company in the UAE to ship the material to an awaiting organization in Iran.[41] And in March 2009, Mahmoud Yadegari procured pressure transducers from a company in Massachusetts and attempted to transport them to Iran through Canada. The transducers have applications in uranium enrichment processes.[42]

The Iranians also use third parties such as the Khan network to acquire needed goods. From the 1980s through 2003, Khan sold Iran centrifuge blueprints, pre-forms, centrifuge assemblies, a number of studies on the production of uranium hemispheres in nuclear weapons, and nuclear weapon designs thought to be based on early Chinese models.[43]

Brazil

There is evidence that Brazil looked outwardly to find the technologies it needed to establish its nuclear program. Some nonproliferation analysts such as David Albright note that it was German manufacturers who helped Brazil establish its nuclear laboratories, design its first centrifuges, and develop a pilot plant at Aramar.[44] Other analysts suspect that A.Q. Khan may have helped Brazil obtain centrifuge designs and equipment for its program. In a 2004 media interview, Henry Sokolski, asserted that Brazil's centrifuges are similar to the P2 centrifuge design sold by Khan's proliferation network to Iran and Libya. Although there may not be enough evidence to suggest that Khan sold the centrifuges to Brazil, the government has not

yet explained where the designs for its centrifuges originated. Brazil claims that next generation centrifuges operating at a Resende commercial sized facility are direct descendants of those at Aramar. In 2004, Brazil's reluctance to explain or exhibit these new technologies led to a diplomatic crisis with the IAEA when Brazilian authorities refused to allow Agency inspectors full access to Resende's enrichment halls. Although Brazil's Ministry of Science and Technology maintains that the rotors used at Resende are entirely indigenous, experts such as Maria Rost Rublee, suspect that Brazil concealed the source of Resende's enrichment technology because it may have indicated illegal or inappropriate procurement activity.

Libya

In the 1990s, Libya contracted with the A.Q. Khan network for the materials needed to develop an indigenous uranium enrichment program. Khan and his network provided the Libyan authorities numerous items including 20 pre-assembled uranium centrifuges and enough components for an additional 200 first generation centrifuges. The network also transferred 10,000 second generation centrifuges and supporting equipment including feed stations, product and tails withdrawal stations, vacuum equipment, cascade piping, drive systems and other miscellaneous equipment. Khan's colleagues helped to manufacture and ship the components and equipment from entities in over 10 countries. In addition, the network provided Libya technical assistance and design information on a conversion and fuel fabrication laboratory; a post-irradiation examination facility, designed for the receipt and disassembly of pressurized water reactor (PWR) spent fuel assemblies ("Project 307"); a radiochemical separation laboratory, consisting of a pilot scale Purex reprocessing plant designed for processing approximately 1100 kg of uranium per year of PWR spent fuel and recovering approximately 10 kg of plutonium per year (referred to as "Project 701"); and a high-level liquid waste vitrification plant, designed for solidifying high-level waste from a reprocessing plant ("Project 303"). Lastly, the Khan network saw to it that Libyan engineers were trained in the use of some of the machines that were provided, and were given design information for the fabrication of a nuclear explosive device, including information related to high enriched uranium re-conversion, casting and machining, and the testing of nuclear weapons components.[45]

Syria

Syria too turned outward for foreign assistance to build its nuclear program. Although the details are not well known, there is evidence that North Korean engineers were in Syria, building a nuclear reactor similar to their own 20-25MWth reactor.[46] To support its contract with the Syrians, North Korea employed one of its own procurement agents to travel abroad

and purchase needed items. According to a *Washington Post* report, Western intelligence tracked the activities of the North Korean company, Namchongang Trading Group (NCG). The company's employees traveled to several European countries such as Germany to purchase an array of items such as electric timers, steel pipes, vacuum pumps, transformers, and aluminum pipes cut to precise dimensions. These items were purchased and shipped to NCG's branch office in Beijing, China, then sent on to the Al-Kibar site.[47] China is a nuclear weapon state, and as such they have different import privileges than non-nuclear weapon states. According to David Albright, "Because it's a branch office in China, NCG can buy equipment from suppliers throughout the world, even in Europe and possibly the United States, particularly if the companies have subsidiaries in China."[48] As Albright pointed out, if items were being purchased at a branch office in China, there may be little suspicion drawn to the transaction.[49]

Similarities in Network Procurement Practices

Looking at known illicit procurement cases, some similarities become apparent. Networks usually start out affiliated with and organized by a state, which gives them the ability to move around the world with ease. They use their nation's embassies as bases for contacting companies that manufacture necessary materials and use expats living in far off lands to procure and ship materials. Networks use educational institutions, companies, and nonprofit organizations as fronts to conceal procurement activities. They also used these fronts to flood suppliers with procurement requests. Networks mislead local authorities by mislabeling items to be shipped and order components then assemble them once reach their ultimate destination. ISIS noted that trading companies are key to illicit procurement networks. These companies barrage multiple suppliers with quotes and purchase requests, often to several offices within the same company and even to subsidiaries in the hopes one order will be filled.[50] They also exploit weaknesses in export control licensing application processes, by undervaluing or mislabeling equipment on invoices and applications, thus avoiding necessary declarations.[51] In some cases, countries, such as North Korea, have created firms that are really fronts. Networks establish logistics routes through allied nations and those with weak export control systems to move acquired goods and hide the location of true end users. Networks also use offshore financial centers to pay for their entire activities.

In some cases, procurement networks emerge as quasi-governmental, semi-independent bodies such as non-governmental organizations, branches of the military, state-owned companies, and nonprofit or religious organizations. The Khan network may be the most flagrant example, but there are others including branches of the Iranian Revolutionary Guard Corps (IRGC) and Iran's Bonyads – organizations that possess an independent authority beyond

the reach of elected officials and other parts of the government,[52] and KAST in Japan. These organizations are often created by the state ostensibly to purchase materials for their programs and usually are given a high level of autonomy. In addition, some of these organizations become both buyers and sellers. Lieggi, Shaw and Toki noted that "Similar to the A.Q. Khan network, which coordinated imports into Pakistan and exports to Iran and Libya, North Korea's WMD-related trade networks have both import and an export sides."[53]

Table 1. Common Illicit Procurement Practices of Networks

	Pakistan	Khan Network	North Korea	Iraq	Iran	Brazil	Libya	Syria
Enlist nationals living abroad	X		X		X			
Send procurement agents around the world looking for material	X	X	X	X	X			
Use embassies and fronts as basis for of procurement				X				
Purchase components rather than full assemblies	X	X	X		X			
Purchase machinery to manufacture needed equipment	X	X	X	X	X			
Mislabel items on shipments	X		X	X	X			
Flood suppliers with requests	X			X				
Pay exaggerated prices for items	X			X				
Transship materials	X	X	X		X			

Use third parties/ networks	**X**		**X**	**X**	**X**	**X**	**X**	**X**

DETERRING AND INTERDICTING ILLICIT PROCUREMENT PROGRAMS

Efforts to deter, interdict, and shut down illicit procurement efforts can essentially be put into two categories: International and domestic. Each has diplomatic, technical, regulatory, and systematic components to them.

International Efforts

International efforts have come in the form of instruments related to trade security and export controls. These include United Nations Security Council Resolutions 1373 and 1540, multilateral export control regimes such as the Nuclear Supplier's Group (NSG) and Missile Technology Control Regime (MTCR), and schemes such as the Proliferation Security Initiative (PSI) and Container Security Initiative (CSI). Some of these are legally binding instruments and some are more informal and voluntary in nature**.** The International Atomic Energy Agency (IAEA), an international body, also has programs and regulations that aid in the verifying and stopping the spread of sensitive technologies. These efforts are discussed below.

UN Security Council Resolution 1373

UNSC Resolution 1373, adopted in 2001, calls for all states to become parties to the relevant international conventions and protocols relating to terrorism, and obliges states to criminalize any assistance to terrorist activities; deny financial support and safe haven to terrorists; and exchange information for the prevention and prosecution of criminal acts. It also emphasizes the need to strengthen a global response to the challenge of illicit trafficking.[54] Although Resolution 1373 does not focus WMD related terrorism specifically, paragraphs 3 and 4 of the Resolution does address terrorist possession of sensitive materials and trafficking in such materials."[55]

UN Security Council Resolution 1540

Adopted in 2004, UNSCR 1540 mandates that states undertake activities to prevent domestic development and dissemination of weapons of mass destruction and their related technologies. These measures include physical protection measures; border controls; actions to detect, deter, and combat illicit trafficking; and export controls. The resolution also obliges all states to adopt and enforce "appropriate effective measures" to prohibit any non-state actor

from manufacturing, acquiring, possessing, developing, transferring, or using nuclear weapons.[56] To help administer activities under UNSCR 1540, the Security Council created a sub-committee - the 1540 Committee - that functions as the repository of the national reports on the implementation of the resolution and helps states acquire the necessary capabilities to complete the objectives of the Resolution.

Export Control Regimes

Four control regimes were developed as informal arrangements to control the transfer of WMD relevant technologies.

The Nuclear Suppliers Group (NSG) is comprised of 46 states, more than half of them nuclear technology suppliers. Regime members adhere to a common set of guidelines to ensure that civilian trade does not facilitate nuclear weapons development. The IAEA publishes NSG guidelines – INFCIRC 254 part I and dual-use export guidelines, INFCIR 254 part II and their revisions as they are updated.

The Missile Technology Control Regime (MTCR) is a group of states that share the goal of controlling the spread of technologies related to missiles, space delivery systems, unmanned delivery systems, and subsystems that could be used to deliver a weapon of mass destruction. Design facilities are also covered in the controls, as are missile related components such as engines, propellants, navigational equipment, and surfaces.

The Australia Group (AG) is an informal arrangement to minimize the risk of spreading material and equipment that may be useful for developing biological and chemical weapons. The Group updates a list of sensitive substances to guide member's control policies, and members agree to use it for that purpose along with a pledge to adopt catch-all controls as a means of controlling sensitive exports to suspect entities.

The Wassenaar Arrangement is an informal agreement between a group of states to control the transfer of conventional weapons and sensitive dual-use goods and technologies. The Arrangement also has an established set of lists of items to be controlled. It promotes transparency and responsibility in trade, and the exchange of information related to the trade of controlled items.[57]

Proliferation Security Initiative (PSI)

The Proliferation Security Initiative (PSI) is a voluntary, informal initiative designed to fill gaps in the multilateral WMD regime.[58] The focus of PSI is to promote cooperation in counter proliferation activities, in particular those focused on stopping the spread of WMD related

technologies. With over ninety members, the PSI has been important in monitoring and interdicting WMD related trade. However, many states (including China) resist joining the initiative due to concerns over the legality of U.S.–led interdiction activities that operate outside the UN framework. Other states are reluctant to adopt the initiative officially because they view it as an unwelcome component of U.S. strategic dominance. Finally, some states are wary of steps that could be construed as a political decision to strategically align with the United States, thus upsetting the fragile balance of power within their region.

The International Atomic Energy Agency (IAEA)

Underlying the entire nuclear nonproliferation regime is of course the Nuclear Non-Proliferation Treaty (NPT). The IAEA implements the activities set for in the NPT. The Agency, established in 1968, serves – to some extent – as an institutional barrier to proliferation activities. Over the years, the IAEA has undergone quite a few changes to attempt to manage the challenges created by new proliferation threats. Nuclear safeguards and nuclear security activities are those that attempt to ensure that nuclear technologies are being used for purposes and the nuclear and radiological materials within a state is secure from malicious acts again it. The IAEA has always played a central role in international efforts to control the spread of nuclear technologies. As noted earlier, the Agency maintains and updates the Trigger List – nuclear material, equipment and non-nuclear materials (INFCIRC/254/Part 1) and Dual-Use List - nuclear-related dual-use equipment and materials and related technology (INFCIRC/254/Part 2). These lists trigger nuclear safeguards at the IAEA and are used as control lists for member states. In 2004, after the Khan network was uncovered and Iran and Libyan illicit activities examined, the IAEA began to investigate potential covert procurement activities around the world. Born out of that activity the Nuclear Trade and Technology Analysis Unit (TTA) – within the Department of Safeguards – it now uses experts in technical and trade issues to analyze any related activities, to support verification activities, and during the preparation of state evaluations. In 2006, TTA launched the Procurement Outreach Program to facilitate states' voluntarily provision of relevant nuclear trade related data. This data includes suspicious procurement inquiries received by companies and on occasion, state authorities have released information on export denials.

Other international organizations such as Interpol and the World Customs Organization have played roles as forums for sharing information about possible illicit procurement activities, educating their constituencies about these activities, and encouraging cooperation within law enforcement activities.

Bi-lateral Arrangements

Across the globe, countries have entered into partnerships to cooperate in areas of information sharing, law enforcement, and interdiction techniques, and assisted partners to strengthen their own national programs. The U.S. has a number of programs to work with international partners to deploy radiation detection systems at international crossing points, airports, and seaports, and to provide mobile systems for use at interior checkpoints to detect and deter illicit transfer of nuclear and other radioactive sources. The U.S. Department of Energy's Confidence-Building Measures Program is advancing international cooperation in nonproliferation nuclear forensics. It applies scientific techniques to identify unique characteristics of nuclear and radioactive material.[59]

Domestic Efforts

So far, nations have applied varying levels of protection against the flow of sensitive materials inside and across their borders. These levels of protection include licensing procedures, border controls, customs regulations, law enforcement techniques, intelligence collection, and analytic activities.

HOW DO NETWORKS CONTINUE TO OPERATE?

With so many controls in place, how do networks continue to operate? It appears that there are numerous gaps in both international and national control activities.

Existential Challenges

New technologies in transportation and communication have both facilitated increases in trade between nations and overwhelmed efforts to detect and interdict the illicit trade of sensitive materials. Globalization, defined as the integration of markets and technologies in a way that enables individuals and corporations to reach around the world farther, faster, deeper and cheaper than ever before, has translated to new methods for moving materials both legally and illegally, which in turn has manifested into exponential growth of world trade and interdependence between nations for all kinds of goods.[60] The evolutionary process has enabled manufacturers to purchase components from one country, assemble them in another, and ship a finished product to yet another country for final use. This new "modular" approach to manufacturing means that very few things are made in one factory anymore, but instead are now assembled from component parts that come from a variety of locations, some national, some international. Law enforcement and export control authorities struggle to keep up with the flow of materials between suppliers and their customers. Authorities also have trouble keeping up with the flow of materials through subsidiary companies that are spread over the

world. The partitioning of corporate functions and offices to remote corners of the world has impeded the monitoring capabilities of law enforcement and other agencies. Thus, globalization albeit a wonderful trend for world economics, and a smuggler's dream, is also law enforcement's nightmare.

Nuclear suppliers have been gearing up for the expansion of nuclear energy around the world. Countries are building nuclear reactors to cope with their future energy needs and to find cleaner means of producing energy. Subsequently, industrial growth may be attractive to procurement networks.

Then there is the profit potential for would be smugglers to move goods from or through their country. Peter Crail, a nonproliferation expert notes that much like other forms of smuggling or highly profitable illegal activity, the profit motive in selling sensitive technologies is too strong to shut down such activities entirely.[61] There appears to always be someone within the firm that is willing to do almost anything for money. According to Crail, "Those who see any potential for profit without getting caught will indeed find ways to circumvent existing controls."[62]

International Challenges

On the international level, export control instruments are limited by four common flaws: first, unclear obligations, many of which are voluntary, therefore are not legally binding; second, there is insufficient agreement on the threat; third there are unsatisfactory standards and disagreement on what standards should be; and fourth, there is inadequate monitoring of implementation and poor use of other existing multilateral tools to support them. For example, although UNSC Resolution 1540 could be an important pillar in protecting against illicit trafficking activity, it has not become that because nations have been slow to implement the resolution's mandates fully. During a 2009 review of the Resolution, experts assessed that there were particularly low levels of implementation in certain areas such as physical protection of nuclear materials, in measures for border and export controls of nuclear-related materials and in all aspects of state enforcement of national controls.

Other international entities often find themselves without authority and unable to take any action if they did find suspected activity. This is the case at the IAEA Department of Safeguards where the TTA investigates suspicious transactions, but is not able to do the intrusive investigation necessary to uncover a network. Even if they did, the IAEA would be not be able to do more than confront a nation and offer up evidence of suspicious activity. The same holds true for the Office of Nuclear Security where the role is not much more than

advisory to the Agency's member states. The IAEA's limited authority is tied to fundamental debates among its member states over interpretation of the threat, what to do about it, and how much control nations are willing to give to the Agency to try to quell the threat.

Another international challenge is in the area of information sharing between nations. Often there is a contradiction between the need to focus on domestic efforts and sharing information to facilitate international counter-proliferation efforts. A stumbling block to sharing internal information regarding nuclear capable individuals and organizations is confidentiality, as this information could be classified from a national security perspective. The public disclosure of such information could make these individuals or organizations targets for proliferators.[63] Additionally, economic difficulties could arise if companies were shut down due to suspicious activities. Without specific proof, national governments may not be willing to make arrests or close businesses until after investigations have been completed.

Domestic Challenges

Although nations have come to some common understanding of the problems that stem from illicit trade and terrorism related activities, they have yet to come to a consensus regarding the seriousness of the threat and what to do about it. Dr. Douglas Shaw at George Washington University asserted that "Illicit trafficking is complex and diverse, and in some cases efforts to suppress one element of illicit trafficking can facilitate other elements of the activity."[64] To be sure, there are a number of issues that impede the control of materials in a country. An example is the way governments are implementing UNSC Resolution 1540. Because some do not agree on the danger that non-state actors pose to them, they do not take the same actions as others to ensure that bad actors are not operating within their borders. This is only partly due to the ambiguity within the language of the resolution regarding its implementation.

Some states believe that efforts to stop proliferation only benefit the interests of established nuclear weapon states and do not serve any larger international interest to prevent nuclear war. This is the classic North-South debate between the nuclear haves and the have-nots. Non-Aligned Movement (NAM) countries have always been sensitive about accepting any policy that may slow down their continued economic development. As noted, some countries are planning for a growing energy demand to support their burgeoning economies. They are doing all they can to increase their energy production capacity, which in most cases has included developing or expanding their nuclear power production capabilities. Any measures that would stall growth would be looked down upon by these nations, and considered a form of

discrimination by developed countries. This may also be the reason that these nations continue to interpret their nonproliferation obligations in ways that they see will not hamper their economic objects. Although it is true that the world is increasingly behaving as though it were a part of a single market, nations still wish to maintain their sovereignty and continue to work to benefit their own economic goals. Some states appear to be concerned about proliferation activities only when they are a direct threat to their own national interests. Therefore, these states pay little attention to curbing international illicit procurement activities.

States may not have the legislative instruments, customs, procedures, or law enforcement resources necessary to fully control firms with relevant knowledge, products, and or technologies. In other countries cultural stigma and distrust of authority minimizes any control over economies and commerce. In still other cases prosecutorial effectiveness can be undermined by the application of local laws that frustrate legal suits against suspects in the gathering of evidence, and limitations of extradition.[65]

Conflicts of interest between government entities may make implementation of controls difficult. In Malaysia for instance, although export controls are aware of their weaknesses, they are working to change their regulations. In their regulatory culture, newly passed legislation has been slow to be accepted by industry or enforced by local agencies.

Still other states have a strong incentive to acquire nuclear weapon technologies or reach a certain level of capability to develop weapons in case they are required.[66] Many believe this is the case of countries such as Japan and Iran.

Network Characteristics

Do the structure and characteristics of networks enable them to continue to operate? According to Albright and his colleagues, "Networks are often small and dispersed within the immense network of global business. The legitimate global market is enormous."[67] Therefore, the job of detecting an illicit network is difficult. Enquiries from smuggling networks are only a tiny fraction of the total number of enquiries a supplier receives. In 2010, a European company calculated that only one-tenth of a percent of all of the inquiries raised red flags.[68] It is no wonder then that it is difficult for some suppliers to discern legitimate from illegitimate enquiries.

Networks are flexible and resilient making their elimination difficult. They can use one trading company, business or contact, then quit using it and move on to another. Networks are always identifying new partners and avenues to do their business. They are also always

changing partners, growing and shrinking, thus making them unfixed, ever changing, and difficult to detect and pin down for any amount of time.[69] Hugh Griffiths noted that "the problem with illicit procurement networks is that many of the actors with whom they engage are actually legitimate companies… In many cases only it's only the apex actors that are knowingly engaged in an illicit procurement network."[70] New suppliers are always emerging in developing markets (countries and regions), that may have varying degrees understanding of the problem, thus causing fluctuations in the overall control of trade.[71] Another characteristic is the adaptability of networks. According to Griffiths "Adversarial networks/actors engaged in the procurement of WMD/dual use goods have adopted the methodologies used by various south and central American cartels/drug trafficking organizations and their partners in Europe."[72] Why? The cartels were faced with the best resources and control regimes and were able to adapt and evolve in order to transport their product and import the precursors that are essential to manufacturing their product.[73] Dr. Paulo Barretto of Texas A & M University added that, "There is not much difference between an illicit nuclear procurement network and any other illicit network, be it on arms trade or drug distribution network. The actors, their motivation and outreach activities are similar."[74] It is also necessary to be honest about the problem and admit (as Crail did earlier) that illicit trafficking of nuclear technologies, just like any other commodity, is profitable. Therefore, there is always going to be great determination by would be suppliers to enter into this business and stay in it, sometimes finding new ways to circumvent existing control. New technologies too could also emerge that would simplify the task of making weapons easier and possibly easier to mask from investigators. Many networks sit behind the veil of government administrations, which makes them even more difficult to identify, understand fully, and disband externally.

Table 2. Problems Of Existing Export Control Regime and Possible Solutions

Existential Challenges (inherent factors stemming from evolving worldwide business and science trends)	**Affect On the Regime**	**Solutions**
• Globalization	• Difficulty to keep track of queries and movement of goods	• Greater cooperation in monitoring, and law enforcement. • Coordination in licensing
• New suppliers entering the market all the time • May not have adequate regulatory structure	• Little or no controls established within the supplier organization • Easy targets for illicit networks	• Lists of companies need updating continuously • Information sharing

• New relevant technologies emerging • May not yet be classified and regulated	• May facilitate weapons development and/or circumvent controls	• Continued monitoring of research into sensitive technologies. • Consulting with partners and relevant control groups to keep them informed. • Apply appropriate regulations to technologies as soon as is appropriate.
• Smuggling is profitable	• Suppliers maybe persuaded to trade	• Increase the potential cost of sales to suspicious buyers: o Blacklists o Suspension from trade if caught o Fines o Longer jail sentences • Increase the possibility of getting caught: o Strengthen licensing procedures o Increase national inspection regime o Better monitoring of sales and rumors of sales
International Challenges	**Affects on the Regime**	**Solutions**
• Inadequate adherence to some international treaties (i.e. 1373 and 1540)	• Gaps in implementation	• Assessments and consultations between the 1540 committee and national representatives
• Unclear obligations	• Gaps in implementation	• Clarify requirements o Define them better o Education and training
• Insufficient agreement on the threat	• Because nations cannot agree on the level of threat against them, they cannot agree on the necessary level of measures to take	• Better sharing of information about the threat • Discuss and come to an agreed level of threat or a matrix describing threat levels
• Some nations see any nonproliferation activities as discriminatory and	• Nations do not fully apply nonproliferation and export control measures	• Consultations between NWS, industrialized states, and NAM • Address nation's issues

inhibiting the growth of their economies		○ Cultural ○ Economic ○ Political • Find compromises ○ Possibly provide incentives (not threats) or sliding scales on measures to take into account economic and culture factors
• Weak national export controls	• Materials flow unregulated	• Assistance and continued partnership ○ Assistance missions ○ Follow-up missions
• Weak legislation	• Legislation has loopholes and not enough strength	• Guidance and assistance from other nations and some international organizations (i.e., IEA, IAEA)
• Weak national customs regulations and law enforcement	• Bad guys are undiscovered or not apprehended	• More assistance from outside entities ○ International Organizations (i.e., Interpol, Europol) ○ Nations (i.e., U.S.A., Japan)
• Competing interests and resources	• Programs are not fully implemented	• Assistance • Education from international organizations and partners
Network Characteristics	**Affects on the Regime**	**Solutions**
• Small and dispersed	• Difficult to detect	• Greater intelligence efforts, watch lists
• Flexible and resilient	• Hard to ascertain the true size or core structure	• Track and analyze data regarding suspicious business activities and entities
• WMD networks have adopted successful smuggling methods or other networks of other commodities (i.e. drugs, humans, etc.	• Difficult to detect or squash	• Work with local and national law enforcement to use analogous methods to stop these networks

STRENGTHENING EXISTING PROGRAMS

There are, of course, various ways to tackle each of the deficiencies that we found while doing this research, but as noted earlier, there is no silver bullet or bullets that if implemented

would shut down all networks or prevent others from being established. However, there are actions that we can take to strengthen current controls and improve the effectiveness of the export control regime. What all these improvements point to is the need for the international community to come to a consensus regarding the threat and the need to tackle it together. What is needed is the development of an international body to standardize levels of control measures internationally, verify the implementation of those measures, and coordinate nonproliferation activities across the board. The preferable method of establishing this body would be to use an existing organization such as the 1540 Committee or the IAEA and give it authority and responsibility for implementing standardization and verification measures. The body could perform objective inspections, monitoring, and report the status of implementation as well as the level of threat internationally. It could also help strengthen regional and national programs to maintain and effective international control regime.

Domestically, government agencies need to cooperate more fully with businesses to stop outside buyers from acquiring sensitive materials. Agencies need to communicate more clearly with businesses to make them aware that they are being targeted by suspicious entities. This approach will help to deter some would-be suppliers from illegal acts, no matter how profitable they may be.

In a war against those who will purchase for others and those who are developing weapons of mass destruction, manufacturers and distributors are on the front line. Economists will confirm that the law of supply and demand will dictate the market, no matter how stringent the rules against selling particular items. If the potential for profits is high enough and the possible risks of getting caught are low enough, criminals and people who are normally honest will find a way lie, cheat, steal, or transfer any goods to a eager buyer. Therefore, what needs to be done is to raise the potential for getting caught buying sensitive goods so they will not do it. Only then will networks stop their attempts to acquire materials in certain areas.

To increase the chance of detecting suspicious enquiries, responsible companies should establish trade control offices and train their personnel to spot suspicious procurement patterns. Identifying suspicious enquiries can improve the chance of early detection of trafficking networks before an order is made or any goods are shipped.[75] According to Albright, “To increase the chance of detecting suspicious enquiries, responsible companies establish centralized trade control offices and train their personnel to spot suspicious procurement patterns. Identifying suspicious enquiries can improve the chance of early detection of trafficking networks before an order is made or any goods are shipped.”[76]

In their report "Internal Compliance Programs," SIPRI analysts note that a central element of a national export control strategy should be to ensure that entities that are involved in the trade of controlled goods are both capable and willing to carry out their activities in accordance with an export control environment. According to the report, "One common method for achieving this goal involves companies putting into place a system that minimizes risks of illegal exports. Such a system is generally referred to as an internal compliance program (ICP) or an internal compliance systems (ICS)."[77] An ICP seeks to: develop contacts and good-standing relationships between the entity and export agencies; stay informed of updates to export control rules and procedures; standardize procedures; provide a centralized forum for export-related questions and issues; provide early warning of possible suspicious enquiries and orders; document all export transactions; and train company employees of the process of fielding inquiries, filling orders, and shipping sensitive materials under established regulations.[78] Governments can help companies set up an ICP that is appropriate for the efficient operation of their organization. Also, governments can work more closely with business to identify and stop clandestine procurement practices. Likewise, business managers need to alert their government counterparts when they receive questionable purchase inquiries. Government agencies can then facilitate interdiction – sometimes with international partners – to make arrests.

CONCLUSIONS

In the illicit trafficking equation, globalization is both a significant part of the proliferation problem and the key to the nonproliferation solution. Improved transportation and communication technologies have increased the flow of materials and money in a way that has caused greater international competition and greater interdependence in regard to their economic health. Therefore, countries are more dependent than ever on each other to make the right choices and stop sales of technologies that would ultimately harm all nations. However, in some nations, political, cultural, and economic factors make fulfilling their international nonproliferation obligations seem like mission impossible.

The illicit trafficking problem cannot be solved by one organization or one country alone. It will take the intent of all nations to stop this activity and coordination among them to stop and prevent illicit procurement networks from operating. Nations need to accept their interdependence more fully and emphasize their efforts to strengthen international nonproliferation norms. These in turn will improve national industrial capabilities. Better implementation of international controls, better coordination among nations, greater cooperation between government and business, and further integration between national

export control and law enforcement agencies are just a few of actions that nations can take to ensure that illicit traffickers are identified and stopped from operating within their borders.[79]

---

[1] As grippingly retold in Richard Rhodes, *Dark Sun: The Making of the Hydrogen Bomb* (New York: Touchstone, 1996).
[2] Sensitive technology can be defined as any technology that may lead to the development of a weapon of mass destruction (WMD).
[3] "Summary of Major U.S Export Enforcement and Embargo-Related Criminal Prosecutions: 2007 to the Present," Department of Justice, January 2012, www.Justice.gov/nsd/docs/export-case-fact-sheet.pdf.
[4] Ibid.
[5] Alexander H. Montgomery, "Ringing in Proliferation," *International Security*, Vol. 30, No. 2, (Fall 2005), p. 170.
[6] Ibid., p 172.
[7] Ashley Nilsen, "The New Face of Illicit Trafficking Networks," presented at *Pacific Northwest International Conference on Global Security – The Decade Ahead,* 2011.
[8] "Nuclear Black Markets," International Institute for Strategic Studies (IISS), 2007.
[9] Mark Hibbs, "The Future of the Nuclear Suppliers Group," Carnegie Endowment for International Peace (CEIP), 2011.
[10] For example, an investigation is underway in Japan, to determine if an unnamed company's sale of a uranium conversion facility to Libya is in violation with Japan's export control laws. Although not handled by middlemen, the transaction reportedly involved other countries, as the packing material originated from outside Japan. "Did Japan Know About Libya Nukes?" CBS News, February 20, 2004.
[11] Bruno Gruselle, "Proliferation Networks and Financing," Foundation for Strategic Research, March 3, 2007.
[12] "Summary of Major U.S Export Enforcement and Embargo-Related Criminal Prosecutions: 2007 to the Present," Department of Justice, January 2012, www.Justice.gov/nsd/docs/export-case-fact-sheet.pdf.
[13] "Illicit Procurement Infrastructure," *Institute for Science and International Security (ISIS)*, May 2003, http://www.exportcontrols.org/print/domestic.html.
[14] "IRAQ'S Silent Allies In Its Quest For The Bomb," *Business Week*, January 14, 1991, http://www.businessweek.com/archives/1991/b319537.arc.htm.
[15] Ibid.
[16] Michael Rietz, "Dual-use Exports, or a Twilight Business Versus Systemic Failures of Export Controls," talk delivered at a luncheon sponsored by the Institute for Science and International Security, (ISIS), December 10, 1999, http://www.isis-online.org/publications/iraq/talkwashforweb.html; Mark Hibbs, "German Expert Wanted by Authorities For Giving Iraqi Carbon Centrifuge Rotors," *Nuclear Fuel*, November 9, 1992.
[17] "Iraq Survey Group Final Report: Executing Illicit Procurement in Iraq: Ministries, Commissions, and Front Companies," October 30, 2004, as posted on Federation of American Scientists (FAS), http://www.globalsecurity.org/wmd/library/report/2004/isg-final-report/isg-final-report_vol1_rfp-03.htm.
[18] Ibid.
[19] "OSC Analysis: Association of Korean Scientists in Japan Reportedly Involved in Proliferation to DPRK," OSC, OSC Doc Id. FEA20060131018507; "Photographic Record of Pro-Pyongyang Koreans in Japan Supporting DPRK, 2002," OSC, May 2006, OSC Doc Id. KPP20060518300003.
[20] Ibid.
[21] Katsuhisa Furukawa, "Japanese Authorities Target North Korean Technology Procurement," *WMD Insights*, November 2007.
[22] "Japan Raid Over Nuclear Exports," BBC News, July 31, 2008, http://news.bbc.co.uk/go/pr/fr/-/2/hi/asia-pacific/7534798.stm.
[23] Ibid.
[24] Dianne E. Rennack, "North Korea Economic Sanctions," Congressional Research Service, Found on Federation of American Scientists Archive, October 17, 2006, http://www.fas.org/sgp/crs/row/RL31696.pdf.
[25] Mark Hibbs and Shahid-ur Rehman, "U-235 Contamination Found On Russian Aluminum Imported by DPRK," *Nuclear Fuel*, July 14, 2008, p. 12; "North Korea Attempted To Procure German-Made Precision Equipment," *Konfidensharu*, July 23, 2008.
[26] "North Korea Attempted To Procure German-Made Precision Equipment," *Konfidensharu*, July 23, 2008.
[27] Ibid.

[28] "Japan to Impose Strictor Sanctions Against North Korea," *Mainichi Interactive*, September 14, 2006; Keiichi Takagi and Hiroshi Kawase, "Japan in Trouble! Part One: The Hidden Enemy" *Sankei Shimbun*, July 21, 2007.
[29] "Illegal Pump Exports to DPRK Reflect Wider Problem," The Daily Yomiuri," June 12, 2008. This revelation came about after the IAEA visited the Yongbyon plant during verification activities earlier this year.
[30] "North Korea Acquiring Banned Japanese Products Through Taiwan as Procurement Base," *Sankei Shimbun*, August 25, 2007.
[31] Lieggi et. al, "Taking Control Stopping North Korean WMD-related Procurement," *Bulletin of the Atomic Scientists*, September 27, 2010.
[32] Catherine Boye, Melissa Hanham, and Robert Shaw, "North Korea and Myanmar: A Match for Nuclear Proliferation?" *The Bulletin of the Atomic Scientist,* September 27, 2010.
[33] Lieggi et. al., "Taking Control Stopping North Korean WMD-related Procurement," September 27, 2010.
[34] Catherine Boye, Melissa Hanham, and Robert Shaw, "North Korea and Myanmar: A Match for Nuclear Proliferation?" *The Bulletin of the Atomic Scientist,* September 27, 2010.
[35] Michael Eisenstadt, *Iranian Military Power: Capabilities and Intentions* (Washington, D.C.: The Washington Institute for Near East Policy, 1996), p.108, cited in Andrew Koch and Jeanette Wolf, "Iran's Nuclear Facilities: a Profile," Center for Nonproliferation Studies, 1998.
[36] *AGIE website*, http://www.agie.com.
[37] "Iranian Entity: Abdollah Nagash Souratgar," *IranWatch-Wisconsin Project*, September 8, 2004.
[38] "Supplier: Eva-Marie Hack," *Iran Watch – Wisconsin Project*, July 21, 2004.
[39] "Summary of Major U.S Export Enforcement and Embargo-Related Criminal Prosecutions: 2007 to the Present," Department of Justice, January 2012, p.p. 15, 16, http://www.justice.gov/nsd/docs/export-case-fact-sheet.pdf.
[40] Ibid., p. 14.
[41] Ibid.
[42] Ibid., p. 29.
[43] Annette Remelsberger, "Staatsanwaltbeschuldigt Iran," *SüddeutscheZeitung*, March 28, 2006.
[44] David Albright, "Bomb Potential For South America," *Bulletin of the Atomic Scientists*, May 1989.
[45] "Implementation of the NPT Safeguards Agreement in the Socialist People's Libyan Arab Jamahiriya," International Atomic Energy Agency (IAEA), September 12, 2008, pp. 3-9.
[46] Paul Brannan, "ISIS Analysis of IAEA Report on Syria: IAEA Concludes Syria "Very Likely" Built a Reactor," Institute for Science and International Security (ISIS), May 24, 2011, http://isis-online.org/uploads/isis-reports/documents/ISIS_Analysis_IAEA_Report_Syria_24May2011.pdf.
[47] Robin Wright and Joby Warrick, "Purchases Linked N. Korean to Syria: Pyongyang Company Funneled Reactor Parts to Damascus, Intelligence Officials Say," *Washington Post,* May 11, 2008, p. A18.
[48] See David Albright and Paul Brannan, "The Al Kibar Reactor: Extraordinary Camouflage, Troubling Implications," Institute for Science and International Security (ISIS), May 12, 2008, http://www.isis-online.org/publications/syria/SyriaReactorReport_12May2008.pdf.
[49] Ibid.
[50] "ISIS Policy Lessons from Illicit Nuclear Trade Case Studies, Institute for Science and International Security (ISIS), 2010, provided by ISIS staff through correspondence in 2011.
[51] Ibid.
[52] Andrew Higgins, "Inside Iran's Holy Money Machine," *Wall Street Journal*, June 2, 2007, http://middleeasttransparent.com/imprimer.php3id_article=3695.
[53] Stephanie Lieggi, Robert Shaw, and Masako Toki, "Taking Control: Stopping Korean WMD-related Procurement," *Bulletin of the Atomic Scientists, 2010.*
[54] National Nuclear Security Administration, "International Safeguards: Challenges and Opportunities for the 21st Century," Office of Nonproliferation and International Security, U.S. Department of Energy, October 2007, p. 41.
[55] Elizabeth Turpen, "Nuclear Security: Key Instruments and Initiatives," Stanley Foundation Working Paper, December 2, 2009.
[56.] "Promoting Nuclear Security: What the IAEA is Doing," International Atomic Energy Agency (IAEA), http://www.iaea.org/Publications/Factsheets/English/nuclsecurity.pdf.
[57] Excerpted from, "Strengthening Multilateral Export Controls," *CITS*, 2002.
[58] For a concise statement of the objectives of the PSI, see the description of the initiative that is provided on the U.S. Department of State website, http://www.state.gov/t/isn/c10390.htm.
[59] Anne M. Harrington, "Fiscal Year 2012 President's Budget Request," May 10, 2011, http://armed-sevices.senate.gov/statement/2011/05%20May/Harrington%2005-10-11.pdf.

[60] T. Friedman, The Lexus and the Olive Tree: Understanding Globalization, 1999.
[61] Peter Crail, personal correspondence, November 23, 2011.
[62] Ibid.
[63] André Buys, "Tracking Nuclear Capable Individuals," Presented at the Workshop on Cooperation to Control Non-State Nuclear Proliferation: Extra-Territorial Jurisdiction and UN Resolutions 1540 and 1373, April 4 - 5, 2011, http://nautilus.org/publications/essays/napsnet/reports/Tracking_Nuclear_Individuals_Buys.
[64] Douglas Shaw, personal correspondence, November 22, 2011.
[65] Binoy Kampmark, personal correspondence November 23, 2011.
[66] Pat Morgan, personal correspondence, November 22, 2011.
[67] David Albright, Paul Brannan, and Andrea Scheel Stricker, "Detecting and Disrupting Illicit Nuclear Trade After A. Q. Khan," *The Washington Quarterly*, April 2010, pp. 90-93.
[68] Ibid.
[69] Ibid.
[70] Hugh Griffiths, personal correspondence, October 12, 2011.
[71] David Albright, Paul Brannan, and Andrea Scheel Stricker, "Detecting and Disrupting Illicit Nuclear Trade After A. Q. Khan," *The Washington Quarterly*, April 2010, p. 90-93.
[72] Hugh Griffiths, personal correspondence, October 12, 2011.
[73] Ibid.
[74] Paulo Barretto, personal conversation, October 7, 2011.
[75] David Albright, Paul Brannan, and Andrea Sticker, "Detecting and Disrupting Illicit Nuclear Trade after A.Q. Khan, *The Washington Quarterly,"* April 2010, www.twq.com/10april/docs/10apr_albrightbrannanstricker.pdf.
[76] Ibid.
[77] Paul Holtorn, Mark Bromley and Lucie Beraud-Sudreau, "Internal Compliance Programmes," *SEESAC*, October 2011, p. 7, http://www.sipri.org/research/armaments/transfers/publications/other_publ/other%20publications/Internal%20Compliance%20Programmes.pdf.
[78] Ibid., p. 8.
[79] John P. Caves, "Globalization and WMD Proliferation Networks: The Policy Landscape," *Strategic Insights,* Volume V, Issue 6*,* July 2006, http://www.npsedu/Academics/centers/ccc/publications/OnlineJournal/2006/Jul/cavesJul06.html.