USAF COUNTERPROLIFERATION CENTER

CPC OUTREACH JOURNAL

Maxwell AFB, Alabama

Issue No. 659, 17 October 2008

Articles & Other Documents:

Welcome to the CPC Outreach Journal. As part of USAF Counterproliferation Center's mission to counter weapons of mass destruction through education and research, we're providing our government and civilian community a source for timely counterproliferation information. This information includes articles, papers and other documents addressing issues pertinent to US military response options for dealing with nuclear, biological and chemical threats and attacks. It's our hope this information resource will help enhance your counterproliferation issue awareness.
Established in 1998, the USAF/CPC provides education and research to present and future leaders of the Air Force, as well as to members of other branches of the armed services and Department of Defense. Our purpose is to help those agencies better prepare to counter the threat from weapons of mass destruction. Please feel free to visit our web site at http://cpc.au.af.mil/ for in-depth information and specific points of contact. The following articles, papers or documents do not necessarily reflect official endorsement of the United States Air Force, Department of Defense,

Washington Post
October 15, 2008
Inside the Ring, Pg. 18

Key Allegations Against Terror Suspect Withdrawn

Justice Department Had Tied Guantanamo Detainee to Plot to Explode 'Dirty Bomb' in U.S.

By Peter Finn, Washington Post Staff Writer

The U.S. Justice Department has withdrawn a series of allegations made in federal court that tie Binyam Mohammed, a British resident held at Guantanamo Bay, to a plot to explode a radioactive "dirty bomb" in the United States, blow up apartment buildings here and release cyanide gas in nightclubs. Defense lawyers said the decision should force the Pentagon to drop charges of conspiracy and material support for terrorism against Mohammed, which were filed by military prosecutors in May. The charges, the lawyers said, are spurious and based on false confessions obtained through torture.

They said the Justice Department dropped key allegations to avoid having to turn over evidence of abuse. The agency did not respond to a request for comment. The dirty-bomb allegation was also never pursued in the case of Mohammed's alleged co-conspirator, Jose Padilla, a U.S. citizen initially declared an enemy combatant but convicted in federal court in August 2007 on a lesser charge of providing material support for terrorism. He was sentenced to 17 years in prison.

"There are no serious, hard charges against Mohammed," said Air Force Lt. Col. Yvonne R. Bradley, his military attorney. "The whole thing the government was hanging its hat on, pursuing Mr. Mohammed, was the dirty bomb." The Pentagon's convening authority for military commissions examines each case assembled by prosecutors before deciding whether it should be referred to a military court for trial at Guantanamo Bay, Cuba. Mohammed's case is "under review," said Joseph DellaVedova, a spokesman for the Office of Military Commissions.

The Justice Department's decision came after a Washington federal judge, in a habeas corpus proceeding, ordered the government to turn over all available exculpatory evidence to Mohammed's attorneys, according to documents filed by government attorneys . The material includes 42 classified British intelligence documents, among them communications with the United States about Mohammed's fate after his arrest in Pakistan in April 2002.

Mohammed's attorneys said they think the documents could shed light on the period between his disappearance in July 2002 and his transfer to the military prison at Guantanamo Bay in September 2004. Mohammed, a 30-year-old Ethiopian native, and his attorneys charge that he was secretly transferred by the CIA to Morocco, where he admitted to various plots only because he was tortured. The High Court in London ordered the release of the documents to Mohammed's attorneys, but the British government argued that they were covered by "public interest immunity" because their release would damage intelligence cooperation and relations with the United States. The British government, however, said U.S. authorities had copies of the documents, effectively transferring any decision-making about their release to Washington. Mohammed's attorneys continue to fight the British government's decision in the High Court.

In the interim, Judge Emmet G. Sullivan of U.S. District Court for the District of Columbia ordered the United States to release exculpatory material by Oct. 6. That day, the Justice Department filed a notice with the court that it was withdrawing assertions contained in its original filing to justify Mohammed's continued detention at Guantanamo Bay. "It's no coincidence that this happened when the judge ordered discovery," said Clive Stafford Smith, one of Mohammed's attorneys and the director of Reprieve, a London-based group that advocates for the human rights of prisoners. "It's clear they think that by dropping the allegations they can avoid having to turn over the documents."

Smith said Mohammed's attorneys would continue to insist in federal court that all documents be disclosed. The United States has allowed one of the lawyers to see seven of the British documents. Their contents are classified, and Smith and other lawyers would not discuss them. The withdrawn section of the Justice Department's original filing deals with allegations that Mohammed planned "to launch a terrorist attack inside the United States." It includes details about alleged discussions by al-Qaeda members on using dirty bombs, using natural gas lines to destroy buildings and releasing cyanide gas. It mirrors the material in the military prosecutors' charge sheet.

"One of the purposes for the attacks on the United States was to help 'free the prisoners in Cuba,' " wrote military prosecutors. Stripped of the core allegations, the government case focuses on Mohammed's training at al-Qaeda camps in Afghanistan. His attorneys don't deny that their client received training in Afghanistan, but they said he wanted to fight in the war-torn Russian republic of Chechnya. Bradley, Mohammed's military attorney, said her client should be returned to Britain, whose government has asked the United States to release him.

Staff researcher Julie Tate contributed to this report.

http://www.washingtonpost.com/wp-dyn/content/article/2008/10/14/AR2008101403146.html?nav=rss_world

(Return to Articles and Documents List)

Christian Science Monitor
October 18, 2008

Bombings of Canadian Pipelines Spark Eco-terrorism Fears

Two explosions in one week cause no injuries, and only minor damage to pipes carrying dangerous hydrogen sulphide gas.
By Arthur Bright

A second gas pipeline bombing within a week in British Columbia, Canada, has raised worries of ecoterrorism in the region, which suffered a similar series of attacks in the late 1990s. The **Globe and Mail** reports that the latest bombing took place near a transfer station owned by energy company EnCana outside Tomslake in northeastern British Colombia, in the same area as another blast that occurred last weekend. Several Royal Canadian Mounted Police (RCMP) units, including the antiterrorism unit, are investigating the explosion, which caused only minor damage.

The first attempt to sabotage an EnCana gas pipeline occurred Saturday night, about 50 kilometres south of Dawson Creek, and the RCMP reported that damage from the second blast, at a nearby location, was discovered yesterday morning. While EnCana described the incident yesterday as "a natural gas leak at a field facility," RCMP Sergeant Tim Shields described it as a second sabotage attempt. "There certainly appears to have been [a bomb]. We have a crater in the ground about four feet across and there is damage to the pipeline. It's dented in. There was also a small leak that was quickly contained by pipeline workers. This is within 20 kilometres of the first incident ... and it has all the earmarks of the first incident," Sgt. Shields said.

"We don't know exactly when it occurred because there were no witnesses who heard the explosion."
The **National Post** reports that police believe the explosions may be related to a letter sent last week to the Dawson Creek Daily News, which demanded "EnCana and all other oil and gas interests" leave Tomslake. "We will no longer negotiate with terrorists which you are as you keep endangering our families with crazy expansion of deadly gas wells in our home lands," the letter said.

The Province reports that at least one expert is calling the explosions acts of terrorism, though police are hesitant to describe them that way, at least for the moment. "Terrorism means the threat or use of violence to influence policy and that's what is happening here," said [Former Canadian Security Intelligence Service lawyer David] Harris, director of international and terrorist intelligence for Ottawa-based Insignis Research. RCMP Sgt. Tim Shields said although he is not using the "terrorism" word, "there is no group or individual that we won't look at."

"We are going on the assumption that the two explosions are linked, given their close proximity and the short time line between the delivery of the note" and the two subsequent blasts, said Shields. John Thompson, president of the Mackenzie Institute, a Canadian thinktank that studies political instability and organized violence issues, told **The Vancouver Sun** that attacks like these have "happened before and will happen again. It's almost like the price of doing business.... The attacks aren't that dangerous, yet. Pipelines break down for other reasons as well. The oil and gas industry is [accustomed] to 'ecotage' and sabotage of various kinds."

Thompson said the style of the attacks appeared rather "amateurish" and he thinks environmentalists would choose other alternatives first rather than planting explosives. If the people involved are not caught, he said, they are gaining experience that could make them more dangerous in the future. "They could keep upping the ante. If not caught, they may learn to do something very spectacular, like arrange a sour gas leak, which could be very lethal," he said.

Although the leak was quickly sealed and didn't cause any injuries, sour gas, as natural gas containing sulphur hydroxide is known, is very dangerous to humans, writes the **Edmonton Journal**. Dawson Creek Coun. Bud Powell worked in the oilpatch for decades and was once struck by leaked sour gas. "At first, it smells like rotten eggs, but then you lose your sense of smell. The next thing you know you're numb and you can't physically move."

Whoever is behind the attacks has to understand the great public risk they could create, Powell said. "You'd have to be deranged to try to do this kind of thing." The National Post notes that the explosions this week are not the first to strike Canada's energy industry. In the 1990s, a series of attacks were made in Alberta, Canada, involving similar threatening letters and bombings. Rancher Wiebo Ludwig was convicted for those attacks and jailed, although he has since been released.

"In the space of two years, there were more than 600 acts of vandal-ism and industrial sabotage, and that was before the bombings – there were as many as six bombings," said Andrew Nikiforuk, who wrote an award-winning book, Saboteurs, detailing the Ludwig story. Mr. Ludwig did not respond to calls for comment yesterday. A woman who answered his phone said she believes he is in Grande Prairie, Alta. Grande Prairie is 100 kilometres from Tomslake.

"Workers have died from sour gas exposures, landowners have lost cattle and horses – on both sides of the border, sour gas is an issue," Mr. Nikiforuk said. "That doesn't justify terrorism of any kind, but it's interesting that the only terrorism we've had in the oil patch in North America seems to be focused on sour gas development." **Mclean's** magazine reported in 1999 that Mr. Ludwig blamed sour gas leaks from pipelines near his home for a variety of ailments his family experienced, including three miscarriages and a stillborn child
.
http://www.csmonitor.com/2008/1017/p99s01-duts.html

(Return to Articles and Documents List)

Unian News Agency
17 October 2008

Pentagon Gives $175 Mln to Ukraine

The U.S. Department of Defense will allocate $ 175 million to Ukraine for struggle against bio-terrorism. According to Delo daily (#189 dated Oct 17, 2008), Ukraine, in its turn, is expected to equip its chemical laboratories, and to create a storage of disease-producing germs. According to the information of the daily, DTRA has already signed a contract with Black&Veatch company, which will develop an electronic disease observations system.

Black&Veatch is about to supply Ukrainian laboratories with new diagnostic equipment able to discover particularly dangerous disease-producing germs, prevent epidemics and potential pandemics caused by a bio-terrorism. Besides, it's also planned to build in Ukraine a constant safe storage for germs on the basis of already existing research institutions.

http://www.unian.net/eng/news/news-279104.html

(Return to Articles and Documents List)

The Times
October 17, 2008

Link Between Child Porn And Muslim Terrorists Discovered In Police Raids

Paedophile websites are being used to pass information between terrorists
Richard Kerbaj and Dominic Kennedy

A link between terrorism plots and hardcore child pornography is becoming clear after a string of police raids in Britain and across the Continent, an investigation by *The Times* has discovered. Images of child abuse have been

found during Scotland Yard antiterrorism swoops and in big inquiries in Italy and Spain. Secret coded messages are being embedded into child pornographic images, and paedophile websites are being exploited as a secure way of passing information between terrorists.

British security services are also aware of the trend and believe that it requires further investigation to improve understanding of terrorists' methods and mindsets. Concerns within the Metropolitan Police led to a plan to run a pilot research project exploring the nature of the link. One source familiar with the proposal said that this could eventually lead to the training of child welfare experts to identify signs of terrorist involvement as they monitor pornographic sites.

Concerns have already been expressed at Cabinet minister level about the risk of vulnerable Muslim youths being exploited by older men. Officers have noted that child sex abuse images have been found during investigations into some of the most advanced suspected plots. However, it is understood that the proposed research project was never implemented because the AntiTerrorism Branch was overwhelmed by the sheer number of cases it was having to deal with.

It is not clear whether the terrorists were more interested in the material for personal gratification or were drawn to child porn networks as a secure means of sending messages. In one case fewer than a dozen images were found; in another, 40,000. British security sources confirmed that such a link had been discovered in several cases. They noted the contradiction between people supposedly devoted to theocracy and Islamic fundamentalism and their use of child pornography. "It shows that these people are very confused," a source said. "Here they are hating Western decadence but actually making use of it and finding that they enjoy this stuff."

Baroness Neville-Jones, Conservative security spokeswoman and former chairwoman of the Joint Intelligence Committee, said: "The information about a possible link between extremism and child pornography potentially provides useful insight into three things: the methods that extremists use to communicate; the methods they use to target vulnerable people in society; and the techniques they seek to use to conceal their online activities." She added: "There is no doubt that these possible linkages should merit further research." Andrew Dismore, the Labour MP and chairman of the parliamentary Joint Committee on Human Rights, said: "This is an important development. We have to do more than just the police work. It needs child protection, criminological and psychological work. It could become a very important weapon in the fight against terrorism." He urged researchers to review cases where terrorists had been convicted to look for this link.

The first British suspicions of a link between child sex abuse and jihadis emerged in London in 2006 when antiterrorism police in two unrelated investigations were shocked to find computerised images of hardcore child pornography. The key case that tipped off the security services to a plausible link involved the "White-chapel Rapist", Abdul Makim Khalisadar. A former Mujahidin and a preacher at the East London Mosque, he was being examined for his links to a hardcore Islamic militant who was later convicted of terrorism. Khalisadar was never convicted of terrorist offences. The other investigation involved a young religiously observant Muslim.

The Times has learnt that a criminal investigation also found child pornography on computers after a raid in 2001 at a mosque run by an al-Qaeda recruiter in Milan. Italian police believe that the images were encoded with messages. At a forthcoming terrorism trial in Spain, the alleged mastermind of a Muslim cell has also been accused of downloading hundreds of child sex abuse pictures and videos.

Meanwhile, police uncovered a right-wing terrorist plot when they raided a home after being tipped off about pornographic images. This June, the Nazi sympathiser Martyn Gilleard was jailed for 16 years after being found guilty of terrorism. Police found 39,000 indecent images of children at his flat in Yorkshire.

Invisible ink for the internet age

— Messages may be concealed within digital images and audio, video or other files. The method is called steganography, derived from the Greek for “covered writing”

— Although the average person will not be able to detect the hidden messages by either listening to or viewing a file, the intended recipients can use applications to reverse the steganography process and gain access to the information

— Experts say that the advancement in encryption technology is outpacing the authorities’ abilities to monitor suspected terrorists and paedophiles

— Italian authorities uncovered files of child abuse images that had been manipulated by a terrorist cell after a raid on the Via Quaranta mosque in Milan in November 2001. Investigators claimed that the terrorist cell encoded the images before sending them to each other

http://www.timesonline.co.uk/tol/news/uk/crime/article4959002.ece

(Return to Articles and Documents List)

Telegraph.co.uk
17 Oct 2008

Terrorists 'Use Child Porn' To Exchange Information

Terrorists may be using child pornography websites to exchange data, according to anti-terror experts.
By Graham Tibbetts

It is thought Islamist extremists are concealing messages in digital images and audio, video or other files. Police are now investigating the link between terrorists and paedophilia in an attempt to unravel the system. It could lead to the training of child welfare experts to identify signs of terrorist involvement as they monitor pornographic websites. The move follows the discovery of sex abuse material during investigations into a number of advanced suspected plots.

It is not clear yet whether the terrorists chose child pornography because of a personal interest or merely because it represents a useful medium for disseminating information. Security officials have been puzzled at the use of such offensive material by people claiming to be devoted to the teachings of Islam. "It shows that these people are very confused. Here they are hating Western decadence but actually making use of it and finding that they enjoy this stuff," a source told the Times.

British police were first alerted to the link in 2006 when they investigated the possible terror links of a former Mujahideen fighter who preached at a London mosque. They discovered computerised images of child abuse. Five years earlier an investigation of a mosque run by an al-Qaeda recruiter in Milan found child pornography that police believe contained encoded messages.

Baroness Neville-Jones, Conservative security spokesman and former chairman of the Joint Intelligence Committee, said: "The information about a possible link between extremism and child pornography potentially provides useful insight into three things: the methods that extremists use to communicate; the methods they use to target vulnerable people in society; and the techniques they seek to use to conceal their online activities."

Andrew Dismore, Labour MP and chairman of the parliamentary Joint Committee on Human Rights, said: "This is an important development. We have to do more than just the police work. It needs child protection, criminological and psychological work. "It could become a very important weapon in the fight against terrorism."

http://www.telegraph.co.uk/news/uknews/3215115/Terrorists-use-child-porn-to-exchange-information.html

(Return to Articles and Documents List)

The Jakarta Post/ The Associated Press

17 October 2008

Analysts: Al-Qaida Has Funds Despite Economic Woes

Sebastian Abbot

Al-Qaida, which gets its money from the drug trade in Afghanistan and sympathizers in the oil-rich Gulf states, is likely to escape the effects of the global financial crisis. One reason is that al-Qaida and other Islamic terrorists have been forced to avoid using banks, relying instead on less-efficient ways to move their cash around the world, analysts said. Those methods include hand-carrying money and using informal transfer networks called hawalas. While escaping official scrutiny, those networks also are slower and less efficient - and thus could hamper efforts to finance attacks.

"It would be inconceivable that large amounts of (terror-linked) money would transit through the formal financial system, because of all the controls," said Ibrahim Warde, an expert on terrorist financing at The Fletcher School at Tufts University. The question of where al-Qaida and its sympathizers get their money has long been crucial to efforts to prevent terrorist attacks. A 2004 U.S. investigation found that banks in the United Arab Emirates had unwittingly handled most of the $400,000 spent on the Sept. 11 attacks. After the attacks, the U.S. made an aggressive push to use law enforcement techniques to disrupt terrorist financing networks and worked with allies to improve their own financial and regulatory institutions.

Al-Qaida and the Taliban have benefited from the drug trade's growth in Afghanistan after the U.S.-led invasion in 2001, and the booming business likely will not be affected by the global slowdown. Opium cultivation has fallen slightly this year but is still about 20 times higher than in 2001, according to the U.N. Office on Drugs and Crime. Former U.S. drug czar Gen. Barry McCaffrey, who recently consulted with U.S. and NATO officials in Afghanistan, issued a report in July saying al-Qaida and the Taliban "are principally funded by what some estimate as $800 million a year derived from the huge $4 billion annual illegal production and export of opium/heroin and cannabis." In addition, wealthy donors and Islamic charities in the oil-rich Gulf, especially Saudi Arabia, continue to be "one of the most significant sources of illicit financing for terrorism," said Matthew Levitt, a former Treasury Department terrorism expert now with The Washington Institute for Near East Policy. The Saudis have long insisted they are doing all they can to rein in terror financing, and U.S. officials have praised their efforts. But, under a system known as "zakat," wealthy Muslims are required to give a portion of their money to the poor. Much of that is given to Islamic charities, and U.S. officials say at least some of that money continues to be channeled to al-Qaida and other terrorist groups.

Saudi Arabia and other Gulf countries have benefited in the last two years from a surge in oil prices from about $60 per barrel at the beginning of 2007 to more than $145 per barrel in the middle of this year. Prices have fallen almost 50 percent in the last few months in response to the global financial crisis, but not before generating hundreds of billions of dollars to oil producers. Levitt said the covert nature of terrorist financing makes it difficult to determine a direct correlation between rising oil revenues and the amount of cash al-Qaida has on hand. But "it stands to reason that if there is more oil revenue, there will be more revenue for all kinds of things licit and illicit," he said. Al-Qaida and other extremist groups have gloated in recent weeks about the West's financial woes, painting the crisis as either divine punishment for supposed wrongs or the last gasps of a dying empire. An American al-Qaida member, Adam Gadahn, said in a video released this month that "the enemies of Islam are facing a crushing defeat, which is beginning to manifest itself in the expanding crisis their economy is experiencing." Members of the militant Palestinian group Hamas and hard-liners in Iran also have cheered the economic turmoil.

Iran is thought to be the last major government supporter of terrorist groups. The majority Shiite country is not believed to finance al-Qaida, a Sunni group, but does support the militant Hezbollah faction in Lebanon, which engaged in war with Israel in 2006. Iran denies the financial crisis is hurting its economy, but falling oil prices will cut into its crude sales, which make up 80 percent of the government budget. It is unclear how that will affect support to Hezbollah. Despite the apparent glut in potential money for terrorist groups, Levitt believes anti-terrorism efforts have hampered their ability to transfer money where they want.

Levitt points to several messages from senior al-Qaida leaders in Pakistan and Afghanistan intercepted by the U.S. or released by the terrorist group itself, asking Gulf supporters for more help because of funding shortfalls. The al-Qaida leader in Afghanistan, Mustafa Abu al-Yazid, appeared in a May 2007 video saying "the mujahedeen of the Taliban number in the thousands, but they lack funds." But Warde and other analysts are not convinced al-Qaida is really hurting. "Anybody who is involved in fundraising of any sort is never going to say we have enough money,

so I think it is a silly argument to say that because there is this intercept ... it is proof that everything we've done has succeeded brilliantly," said Warde.

http://www.thejakartapost.com/news/2008/10/17/analysts-alqaida-has-funds-despite-economic-woes.html

(Return to Articles and Documents List)

Reuters India
17 October 2008

Taliban May Give Up Al Qaeda, Ex-Minister Says

By Sean Maguire

KABUL (Reuters) - The Afghan Taliban could cut its ties with the militant al Qaeda group it once harboured as part of a peace agreement in Afghanistan, a former foreign minister for the austere Islamist movement said on Wednesday. But severing links with the radical Islamists behind the Sept 11, 2001, suicide attacks on the United States should not be a pre-condition for talks between the Taliban and the Afghan government, Wakil Ahmed Muttawakil said.

"Al Qaeda were in Afghanistan before as guests of the Taliban. Now they are allies in the fight," Muttawakil told Reuters. "Al Qaeda will not be allowed to create an obstacle ... it is the right of Afghans to negotiate for peace."

Muttawakil was part of a group of Afghans that met in Saudi Arabia last month for discussions on how to end the worsening conflict between the Taliban and the Western-backed Afghan government, now in its eighth year. All sides agree there were no direct Taliban representatives present or that real peace talks took place in Mecca. But the start of efforts to find a negotiated solution has been seized on as a glimmer of hope amid the rising death toll in Afghanistan.

Muttawakil does not speak directly for the Taliban but is known to retain ties to the movement that ruled most of Afghanistan from 1996 to 2001. It was toppled by U.S.-led and Afghan forces for refusing to hand over al Qaeda leaders.

CONFIDENCE-BUILDING

Muttawakil, known as a moderate in the hardline Taliban, surrendered in southern Afghanistan in 2002 and spent nearly two years in a local U.S.-run prison. Talks would not start unless pre-conditions, such as the rejection of al Qaeda or the Taliban demand that all foreign forces leave, are set aside, he said. "Negotiation is a tool for agreement and agreement is the objective. Neither side should impose pre-conditions on starting peace talks as pre-conditions would hamper the start of negotiations."

U.S. officials have given cautious backing to talks, provided al Qaeda is not part of them, the Taliban agrees to respect the Afghan constitution and Afghanistan remains intact. Afghan President Hamid Karzai has asked Saudi Arabia to mediate with his opponents and made a direct appeal to Taliban leader Mullah Mohammad Omar to return home and talk, a plea rejected by a senior Taliban figure. Diplomats say it will be enormously hard to get a clear answer from the loosely-organised Taliban movement, whose leaders are in hiding and which is backed by other radical groups, drug smugglers and criminal gangs operating on their own agenda. Muttawakil said confidence-building measures were needed. The release of prisoners held by U.S. forces, the end of bounty hunting for Taliban leaders and taking key figures off black lists would be a start, he said.

http://in.reuters.com/article/southAsiaNews/idINIndia-35984620081015

(Return to Articles and Documents List)

GovExec.com
October 15, 2008

DHS Secretary Pushes Industry To Invest In Cybersecurity

By Jill R. Aitoro jaitoro@govexec.com

If industry fails to team with the federal government to address national cyber concerns, consumer trust could deteriorate, bringing dire consequences like the recent fallout in the financial market, said Homeland Security Secretary Michael Chertoff on Tuesday. Reports estimate that industry owns and operates more than 85 percent of the United States' critical infrastructure, which makes cybersecurity a shared responsibility between government and the corporations that control most computer networks, Chertoff said during a forum at the U.S. Chamber of Commerce.

"The failure in even one component, or one link in the chain, can have cascading effects," he said. "Just look at what's going on in the financial market, which is a too dramatic illustration of what happens when there's a failure of trust. ... If ordinary consumers lose confidence in the systems, business suffers and fails." As attacks increase in frequency, sophistication and scope, Chertoff said, government will focus on three areas:

- Cyber threat detection and mitigation, primarily through the second and third generations of Einstein, an automated system that collects, correlates, analyzes and shares computer security information.
- Education on policies and practices to help reduce insider threats.
- Improving safeguards in the global supply chain to ensure computer components delivered to federal agencies are free of vulnerabilities that could expose systems to attacks.

The latter effort, in particular, requires a partnership between industry and government. No one "can presume that in every country they keep commercial interests separate from national interests," Chertoff said. "We need to come up with ways to validate the security of hardware and software. Private industry has begun initiatives to inject quality controls. Government won't come up with a kind of FDA for computer components [that regulates the market], but we can encourage these types of efforts." DHS also plans to work with industry to improve existing cybersecurity efforts. In May 2007, the department announced completion of 17 sector-specific plans under the National Infrastructure Protection Plan, which defines roles and responsibilities for all levels of government and private industry in case of a terrorist attack or disaster. Each set of guidelines is customized to address the unique risks of a particular field, such as the chemical industry, or nuclear reactors, materials and waste. DHS will collaborate with each sector to identify cyber risks and work with corporations and organizations to establish priorities and milestones that can help chart progress. "This is an invitation, not a mandate. We're not in the business to say to industry, 'You must do this,' " Chertoff said, noting that federal funding is not readily available to finance private sector cybersecurity initiatives. "[But] I have no doubt lawyers will tell clients that it would behoove them to make these investments."

http://www.govexec.com/story_page.cfm?articleid=41203&dcn=e_gvet

(Return to Articles and Documents List)

McClatchy-Tribune News Service
October 17, 2008

Safeguarding Our Cyber Borders

By Melissa Hathaway

London shoppers who bought groceries with bankcards over the last two years paid a higher price than they bargained for. Cyber thieves had implanted unauthorized circuitry in keypads sold to supermarkets in the Barking and Dagenham area of the British capital. The corrupted keypads were then used to capture account information and Personal Identification Numbers (PINs). The data were siphoned off and used to skim from or in some cases empty shoppers' bank accounts. The thieves covered their tracks by encrypting the numbers they stole, then storing them on a computer server abroad. It took more than a year for the authorities to catch on.

Stories such as that aren't only sobering news for consumers. For folks charged with securing and protecting the nation's defense and intelligence infrastructure, however, increasingly sophisticated cyber assaults are a chilling -- and increasingly familiar -- challenge. The same devices that thieves use to sneak into bank accounts, the same techniques that hackers use to disrupt Internet service or alter a digital profile, are being used by foreign military and spy services to besiege information systems that are vital to our nation's defense. Because defense and other

national security contractors share data and systems with their government partners, an attack on one can be an attack on many. Plans are only as secure as the weakest link in the information chain. These days, those links are being tested as never before.

The attackers' goals fall into three categories:

• Information theft. Stealing data from a target personal device, system or network is the most common threat. For example, a disgruntled Boeing employee was charged last year with lifting more than 320,000 sensitive company files by using a thumb drive to tap the corporate system. Boeing estimated that the stolen documents would have cost it between $5 billion and $15 billion in lost revenue had they been given to competitors.

• Information disruption. Hackers who sneak into government systems and alter crucial operating data are a growing concern. In 2006, a disgruntled Navy contractor inserted malicious code into five computers at the Navy's European Planning and Operations Command in Naples, Italy. Two computers were rendered inoperable when the program was executed. Had the other three computers been knocked offline, the network that tracks U.S. and NATO ships in the Mediterranean Sea and helps prevent military and commercial vessels from colliding would have been shut down.

• Information denial. Cases in which private or government computer systems are shut down by floods of automated hits are also on the rise. In April 2007, Russian nationalists used such a "distributed denial of service" attack to block access to the networks of the Estonian parliament, the president's office and many of that country's banks, news organizations and Internet service providers.

The "What Ifs" are an even greater concern. Could an adversary insert erroneous data that would cause weapons, early warning systems and other elements of national security to fail at critical times? What if financial or medical records were altered, or rail or air traffic control systems were corrupted? What if malicious code were secretly installed during the manufacture or shipping of computer equipment, to be activated at some future date? How would we even know what threats we face?

Defensive measures are being taken. In January, President Bush proposed a 12-point Comprehensive National Cybersecurity Initiative whose solutions range from a public awareness campaign to sophisticated new systems for identifying and deterring intrusions. Congress approved funding in late September. A key element of the plan -- reducing the number of access points between federal agencies and external computer networks -- is under way. The federal government has closed about 3,500 such access points this year, leaving about 1,000 still open. The goal is to reduce the final number to fewer than 100. Much more needs to be done, however.

We need stronger international alliances to share the responsibility for securing cyberspace. We must do more to convince our allies and strategic partners of the benefits to them of taking an active role. We also need a fundamental re-thinking of our government's traditional relationship with the private sector. A high percentage of our critical information infrastructure is privately owned, and industry needs to know what government knows about our adversaries' targets and, to the extent we understand them, their methods of operation.

When it comes to cyber security, government and the private sector need to recognize that an individual vulnerability is a common weakness. There's time, though not unlimited time, to get the job done. We must make a continuing public commitment to securing cyber space -- and we must do so now.

Melissa Hathaway is the cyber coordination executive for the director of national intelligence. The Department of Homeland Security has designated October National Cyber Security Awareness Month.
http://www.dni.gov/press_releases/20081017_release.pdf

(Return to Articles and Documents List)

Houston Chronicle
October 16, 2008

High-Security Research Labs Not So High Security

By LARRY MARGASAK Associated Press Writer

WASHINGTON — Intruders could easily break into two U.S. laboratories where researchers handle some of the world's deadliest germs, according to congressional investigators. The Associated Press identified the vulnerable lab locations as Atlanta and San Antonio. The serious security problems at the two labs were described by the Government Accountability Office in a report expected to be released publicly as early as Thursday. The GAO, Congress' investigative and auditing arm, did not identify the labs except to say they were classified as Biosafety Level 4 facilities, but the report included enough details for the AP — and others knowledgeable about such labs — to determine their locations.

Biosafety Level 4 labs conduct research on deadly germs and toxins. In Texas, the Southwest Foundation for Biomedical Research features an outside window that looks directly into the room where the deadly germs are handled. The lab, which is privately run, also lacks many security cameras, intrusion detection alarms or visible armed guards at its public entrances. Officials there said they will tighten security. "We already have an initiative under way to look at perimeter security," said Kenneth Trevett, president of the lab in San Antonio. "We're waiting for additional input but we're not waiting long. The GAO would like us to do some fairly significant things. They would like us to do it sooner rather than later."

The other lab described with weak security in the report is operated by Georgia State University in Atlanta. That lab lacked complete security barriers and any integrated security system, including any live monitoring by security cameras. During their review, investigators said they watched an unidentified pedestrian enter the building through an unguarded loading dock. "Georgia State clearly wants its BSL-4 to be as safe as possible," said DeAnna Hines, assistant vice president for university relations. "We are already taking steps that will enhance the lab's safety and security standards." Hines did not confirm the school's research lab was the one mentioned in the congressional report as lacking proper security.

Investigators said the lab in San Antonio used unarmed guards inside antiquated guardhouses with a gate across the access road. An outside company monitors alarms at the lab and calls police in emergencies, which investigators said could delay a quick response in a crisis. They called the San Antonio lab the most vulnerable of all the labs they studied. The federal Centers for Disease Control and Prevention approved the labs in San Antonio and Atlanta to handle the deadly organisms despite the security weaknesses. The three other BSL-4 labs in the U.S. feature impressive security, the report said. Those include the CDC's own facility, also in Atlanta; the Army's lab at Fort Detrick, Md.; and the University of Texas Medical Branch in Galveston.

Fort Detrick is on a secure military base, but it is known for a recent internal problem. Bruce Ivins, a scientist at the Army's biodefense lab at Fort Detrick, killed himself in July as prosecutors prepared to indict him for murder in the anthrax letter attacks, which killed five people. The CDC lab is on the agency's high-security campus. The viruses researched in the highest security labs include ebola, marburg, junin and lassa. All can cause incurable illnesses.

The chairman of the House Energy and Commerce Committee, Rep. John Dingell, D-Mich., urged the CDC to quickly identify all security weaknesses at the high-containment research labs and fix any problems. Dingell has been investigating security problems associated with such labs around the country. He said at least six additional high-containment labs are under construction. The Associated Press reported in October 2007 that U.S. laboratories working with deadly organisms have experienced more than 100 accidents and missing shipments since 2003 — and the number is increasing as more labs do the work. A CDC spokesman, Von Roebuck, said each of the five labs described in the new report has its own security plan designed to fit the lab's particular security assessments.

http://www.chron.com/disp/story.mpl/ap/tx/6061799.html

(Return to Articles and Documents List)

The Hindu
October 12, 2008

India ‘Encourages’ U.S. Nuclear Cooperation With Pakistan

Siddharth Varadarajan

New York: In a statement that marks a significant shift in India’s public attitude towards the prospect of Pakistan entering into nuclear agreements with other countries, External Affairs Minister Pranab Mukherjee said on Friday that he was in favour of the United States cooperating with Islamabad in the civil nuclear area.

Asked at a news conference in Washington shortly after the signing of the 123 Agreement about his views on possible nuclear cooperation between Pakistan and the U.S. and China, Mr. Mukherjee said India would encourage greater use of civil nuclear energy by its neighbour. “In respect of civil nuclear cooperation between Pakistan and the U.S., we would like to encourage civil nuclear cooperation — its full use of nuclear energy — as we believe every country has its right to use nuclear energy for peaceful purposes.

The Minister also praised the recent remarks made by Pakistan President Asif Ali Zardari following his meeting with Prime Minister Manmohan Singh last month.

He did not identify the remarks but Indian officials have welcomed statements made by the Pakistani President in an interview to the Wall Street Journal that Islamabad did not feel threatened by India.

“The recent statement issued by President Zardari is really encouraging and there is no reason of any apprehension by Pakistan,” he said. “India’s commitment to non-proliferation is second to none and we have, in my 5 September statement, reiterated our continuation of the voluntary moratorium [on testing] which we declared in 1998.”

http://www.thehindu.com/2008/10/12/stories/2008101260660800.htm

(Return to Articles and Documents List)

Wall Street Journal
October 15, 2008
Pg. 14

Seeking Funds, Pakistan Turns To 'Strong' Ally China

By Shai Oster and Jason Leow in Beijing, and Matthew Rosenberg in New Delhi

Pakistan's president Asif Ali Zardari began a four-day state visit to China on Tuesday, seeking aid for his near-bankrupt nation from an increasingly powerful ally. "China is the future of the world," Mr. Zardari, widower of slain former Prime Minister Benazir Bhutto, told Chinese state news agency Xinhua on the eve of his trip. "A strong China means a strong Pakistan." Pakistan's economy was already in a critical state before the global financial crisis. Mr. Zardari is reaching out to China, the U.S. and Saudi Arabia, among other so-called Friends of Pakistan, to make the case that the world has an interest in helping to stabilize the nuclear-armed nation, which has been shaken by Islamist militancy.

Pakistan is seeking $5 billion to $6 billion from donors. Government officials are urgently trying to shore up dwindling foreign-exchange reserves -- now down to $8.32 billion -- and revive the ailing economy by boosting the confidence of foreign investors. It sees China as a substantial source of this capital. On his first official visit abroad since taking office, Mr. Zardari promised to return to China every three months and said the relationship would focus on business. Shaukat Tarin, economic adviser to Pakistani Prime Minister Yousuf Raza Gilani who was in Washington early this week, said Pakistan had secured $1.4 billion from the World Bank, and expected additional financing from the Asian Development Bank.

The U.K., meanwhile, doubled its aid to Pakistan and will give the country about $825 million over the next three years, according to the British High Commission in Islamabad. But China may offer Islamabad its best hope for a major cash infusion. The Asian giant's foreign-exchange reserves are the world's largest, at $1.9 trillion. Chinese officials could be eager to demonstrate their new wealth and diplomatic heft, analysts say. "China is already involved in building a large port in Pakistan. But neither Chinese nor Pakistani officials have offered details of any current aid agreement.

The decades-long friendship between China and Pakistan is grounded in arms sales, energy assistance and an all-weather geopolitical alliance. China has sold conventional weapons and missile technology, and is suspected of helping Pakistan develop nuclear weapons. In 2006, China and Pakistan signed a pledge to increase bilateral trade to $15 billion a year by 2011.

As India and the U.S. have worked to complete a civilian nuclear agreement, China and Pakistan have discussed a similar deal. A Chinese foreign-ministry spokesman said there would be "in-depth discussions" on cooperation in

"some major areas," but declined to confirm if a nuclear deal was in the works. Xinhua, quoting the Pakistani foreign ministry, said China and Pakistan expect to sign "several agreements" during Mr. Zardari's visit.

Pakistan's ties with the U.S. remain fraught with tensions. Mr. Zardari has reached out to U.S. leaders, but in doing so has faced criticism at home, particularly because of repeated U.S. missile strikes inside Pakistani territory targeting Islamist militants near the Afghanistan border. An economic collapse would only further undermine the battle against Islamic militants, experts warn.

http://wsj.com/article/SB122400985382133155.html

(Return to Articles and Documents List)

Washington Times
October 16, 2008
Pg. B1

Inside The Ring

By Bill Gertz

Congress voted recently to approve $5 million for a study of space-based missile defenses, the first time the development of space weapons will be considered since similar work was canceled in the 1990s. Appropriation of the money for the study was tucked away in a little-noticed provision of the Continuing Resolution passed recently by Congress and followed two years in which Congress rejected $10 million sought for the study. Sen. Jon Kyl, Arizona Republican and a key supporter of missile defenses, said approval of the study highlights the need to provide comprehensive protection from the growing threat of missile attack and to limit the vulnerability of vital satellites to attack.

"We have the potential to expand our space-based capabilities from mere space situational awareness to space protection," Mr. Kyl said in a Senate floor speech. "In the past 15 years, the ballistic missile threat has substantially increased and is now undeniable," he said on Sept. 29. A total of 27 nations now have missile defenses, and last year, over 120 foreign nations fired ballistic missiles, he said. North Korea and Iran both are developing missiles and selling the technology for them, he added.

Mr. Kyl also said the Pentagon's annual report expressed concerns about accidental or unauthorized launches of long-range missiles from China and about the growing vulnerability of vital satellite systems to attack by anti-satellite weapons, as shown by China's 2007 anti-satellite weapons test. Mr. Kyl said he hopes Defense Secretary Robert M. Gates, who will choose what government or private-sector agency will conduct the study, will choose the Institute for Defense Analyses, a federally funded research center, to carry out the study.

A Senate report on the study stated that independent groups that could produce it include Energy Department national laboratories, or scientific and technical organizations. A defense official said space-based missile defenses were last considered during the first Bush administration as part of its Global Protection Against Limited Strike, or GPALS, a missile-defense plan focused on then-Soviet missiles using a combination of ground-based interceptors, sea-based missiles and space-based interceptors. The Clinton administration canceled all work on space-based missile defense and focused instead on tactical defenses against short-range missiles.

The current Bush administration's missile-defense program is limited to the deployed ground-based interceptors in Alaska and California and ship-based interceptor missile defense. The defense official, who spoke on the condition of anonymity, said space-based defenses are needed for global, rapid defense against missiles. "It's really the only way to defend the U.S. and its allies from anywhere on the planet," the official said.

Afghan report

A military officer in Afghanistan says the threat from improvised explosive devices, IEDs, is real and growing as a combination of insurgents and other armed factions continue to pose a major challenge to U.S. and allied efforts to help stabilize the country. The threat landscape is wide and varied and includes the ousted Taliban and al Qaeda members in addition to warlords and drug-trafficking militia groups. "You have rival political factions that are very tribal based, and the tribes here are a complex milieu ethnically and by clans and families," the officer said. "You also have blood feuds that feed into some anti-government forces."

Add to the mix the $4 billion yielded annually by the Afghan opium trade and the equivalent of South American drug cartels with armed forces who hold anti-government political views, and the situation becomes even more complex, the officer said. U.S. and foreign embassies and Afghan government facilities in Kabul are highly fortified like "Fort Apache," the officer said. "The IED threat is real and growing, along with the occasional rocket," the officer said. The biggest challenge to stabilizing Afghanistan is developing institutions from the national level down to the local level, something that is likely to take 20 years. "For perspective, imagine Afghanistan postured like Cambodia only a few years removed from the killing fields," he said, referring to the post-Vietnam War massacres carried out by the Cambodian communist Khmer Rouge. "We are dealing with not even basic literacy across large swaths of the population."

China missile defense

China appears to be secretly working on the development of strategic missile defenses, China military affairs specialist Richard Fisher states in a new book on China's military modernization. Mr. Fisher states in "China's Military Modernization: Building for Regional and Global Reach," out this week, that reports from China indicate that China continued work on an anti-ballistic-missile (ABM) system that was supposedly halted after development in the 1960s. China's anti-satellite missile, the SC-19, is likely part of the ABM system, and unlike the fixed interceptors used in the U.S. ABM system, the Chinese ABM will use mobile missiles like the SC-19, he states.

Chinese ABM programs are an indication that China's diplomatic efforts to ban weapons in space are a "propaganda campaign intended to limit or delay defensive programs of others," the book states. Mr. Fisher, vice president of the International Assessment and Strategy Center, compiled more than a decade of interviews and Chinese data for the book, which has some provocative findings.

For example, Mr. Fisher estimates that China is moving toward an expanded nuclear force of 120 missiles that, with multiple warheads, could give China a force of up to 500 warheads. Other Chinese goals are space-warfare weapons, advanced combat jets, aircraft carriers and large amphibious forces, he wrote. "What the current American leadership, both in the military and intelligence community, is not telling us is that China is on a track to become a global competitor with the U.S. in the 2020s," Mr. Fisher said in an interview. "By that time, they will be well on their way to assembling all the elements of global power that we have today, and we need to prepare for this threat now." Chinese Embassy spokesman Wang Baodong had no immediate comment on the book or China's missile defenses.

Iran nuclear program

A private nuclear-arms watchdog group issued a report this week that concludes that Iran will have the capability of creating a "virtual" nuclear weapon in January. The assessment by the Wisconsin Project on Nuclear Arms Control states that Iran has a bank of centrifuges that are producing low-enriched uranium that can be used for nuclear reactors but that also can be recirculated through the centrifuges to make bomb fuel.

"The re-circulation raises the concentration of the uranium isotope U-235, which fissions in nuclear weapons such as the one dropped on Hiroshima," the group stated in a report made public Wednesday. "Based on the amount of low-enriched uranium Iran has stockpiled, and the amount it is believed to be producing each month, the Wisconsin Project estimates that by inauguration day, Iran could have enough U-235 to fuel one bomb quickly," the report said, noting that the time frame would be two to three months to raise the level of U-235 from 3.8 percent enrichment to 90 percent. Iran's government has denied that its uranium-enrichment program is directed toward building weapons, and there is no firm evidence that the country has mastered the technology to weaponize enriched uranium.

Bill Gertz covers national security affairs.

http://washingtontimes.com/news/2008/oct/16/inside-the-ring/

(Return to Articles and Documents List)

China-Russia: Guns and Games of August: Tales of Two Strategic Partners

by Yu Bin

The third quarter was quite eventful for Russia and China as well as their bilateral relationship. The Beijing Olympics opened and concluded with extravaganzas. Shortly before the opening ceremony, Georgia's attacks against South Ossetia led to Russia's massive military response and Russia's recognition of their independence. One consequence of the Georgian-Russian war is that China's "neutrality" is widely seen as causing a crisis in China's strategic partnership with Russia. Beyond the Olympics, South Ossetia, and chaos in world financial markets, Moscow and Beijing were able to move their relationship forward with several bilateral agreements.

For full text see: http://www.csis.org/media/csis/pubs/0803qchina_russia.pdf

(Return to Articles and Documents List)

Homeland Security Affairs
October 2008

New Requirements for a New Challenge: The Military's Role in Border

Bert B. Tussing

ABSTRACT: U.S. border security is not what it used to be. Over the last three decades America's concerns have steadily escalated from what was once as much a humanitarian issue as a security issue, to concerns over paramilitary violence, organized crime, and international terrorism. The requirements to meet these concerns have likewise increased, to the point that anything less than an interagency and intergovernmental response will inevitably leave the nation's citizenry vulnerable to a new and expanding series of threats. The new threats portend a new challenge for the military, both active and reserve components. From the United States Northern Command through to the individual state's National Guard our leadership will be required to revisit its thinking, motivation, and ethos in addressing this particular "law enforcement" requirement. It will require our government to decide which entities from the depth and breadth of its capabilities are best postured, best equipped, and best trained to meet the trials that lay ahead.

For full text see: http://www.hsaj.org/?article=4.3.4

(Return to Articles and Documents List)