



USAF COUNTERPROLIFERATION CENTER

CPC OUTREACH JOURNAL

Maxwell AFB, Alabama

Issue No. 708, 01 May 2009

Articles & Other Documents:

[Obama Action Expected Soon on UAE Nuclear Pact](#)

[Extremists said to be Eyeing Somalia as New Base](#)

[Torture Tape Delays U.S.-UAE Nuclear Deal, say U.S. Officials](#)

[Al Qaeda No. 2 Ayman al-Zawahiri calls the Shots, says State Department](#)

[US Can Make Sure Pak Nukes are Secure: Obama](#)

[US Fears Over al-Qaeda in Pakistan](#)

[Safety of Pak Nukes: Obama does not Rule out Intervention](#)

[U.S. Steps Up Effort on Digital Defenses](#)

[China Rejects Japan's Accusation over Its Nuclear Policy](#)

[The Cyber Defense Perimeter](#)

[Swine Flu Vaccine may be Available in 6 Months - Russian Expert](#)

[China: Open about Nuclear](#)

[Swine Flu: Virus may be on Decline in Mexico](#)

[N. Korea Raps Japan over Stalled Nuclear Talks](#)

[Many States Do Not Meet Readiness Standards](#)

[North Korea Threatens New Nuclear, Ballistic Missile Tests](#)

[A Vaccine Needed for Bad Statistics: Eric Auchard](#)

[N. Korea Reaffirms Boycott of Nuclear Talks](#)

[Bin Laden is Dead, Again](#)

[N. Korea Issues Threat on Uranium](#)

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 chemical, biological, radiological, and nuclear (CBRN) threats and countermeasures. 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, or other US government agencies. Reproduction for private use or commercial gain is subject to original copyright restrictions. All rights are reserved.

Forbes.com
Thomson Reuters
April 29, 2009

Obama Action Expected Soon on UAE Nuclear Pact

By Doug Palmer

WASHINGTON, April 29 (Reuters) - President Barack Obama is expected to soon certify a nuclear energy agreement with the United Arab Emirates, setting the stage for action in Congress on a pact that could be worth billions of dollars to U.S. companies, a U.S. business official said on Wednesday.

Danny Sebright, president of the U.S.-UAE Business Council, told Reuters he expected Obama to issue a presidential determination that the agreement, signed in the last days of the administration of former President George W. Bush, is in the best interests of the United States.

That would set the stage for U.S. Secretary of State Hillary Clinton to formally notify Congress of the United States' intention to enter into the nuclear energy cooperation deal with one of Iran's neighbors, giving lawmakers 90 days to vote down the pact if they choose, he said.

'No vote of approval is required. It's just required to sit there 90 days,' Sebright said.

The UAE is best known in the United States for the furor that erupted in Congress several years ago when state-owned Dubai Ports World acquired several U.S. port assets as part of its purchase of British company P&O. DPW ultimately agreed to sell the assets when many Republicans and Democrats objected to an Arab-owned company operating U.S. port facilities.

The incident derailed efforts between the United States and the UAE to negotiate a free trade agreement.

Even so, the UAE last year surpassed Israel as the United States' largest export market in the Middle East.

TIES WITH IRAN

UAE's trade ties with Iran and a gruesome video that appears to show a member of the Gulf Arab state's ruling family torturing an Afghan grains trader could color the debate in Congress over the nuclear deal.

The video, aired last week by U.S. network ABC, shows the Afghan being abused with an electric cattle prod, beaten with whips and a plank of wood with a nail in it, and driven over by a car in a desert location in 2004.

The Abu Dhabi Justice Department said on Wednesday it had launched an investigation and 'unequivocally condemns the actions depicted on the video.'

The UAE was the world's third largest oil exporter in 2007, and Iran the fifth, according to U.S. government figures.

Sebright said the UAE wants U.S. assistance in building a number of nuclear reactors to meet an expected need for an additional 40,000 megawatts of electricity by 2017.

U.S. nuclear reactor builders, GE and Westinghouse Electric Co, a subsidiary of Toshiba Corp, stand to get a big share of the expected \$40 billion market if Congress does not block the deal.

Representative Howard Berman, chair of the House of Representatives Foreign Affairs Committee, said in January Congress would carefully examine the agreement to make sure it would not help Iran develop a nuclear bomb.

Representative Ileana Ros-Lehtinen, a Republican, also is expected to raise concerns about past problems with illegal transshipment from UAE to Iran.

Sebright said he believed those concerns could be addressed because the UAE, by renouncing uranium enrichment and reprocessing of spent fuels, has made clear 'they have no intention of ever wanting a nuclear weapon.'

When the UAE embarked on plans to develop a nuclear energy program, they set out 'to create a clear alternative to the path Iran is taking in the region' and a number of safeguards to prevent spent nuclear fuel from being used to build weapons are part of the pact with the United States, he said.

(Editing by Mohammad Zargham)

<http://www.forbes.com/feeds/afx/2009/04/29/afx6357821.html>

[\(Return to Articles and Documents List\)](#)

CNN.com

29 April 2009

Torture Tape Delays U.S.-UAE Nuclear Deal, say U.S. Officials

By Elise Labott

CNN State Department Producer

WASHINGTON (CNN) -- A videotape of a heinous torture session is delaying the ratification of a civil nuclear deal between the United Arab Emirates and the United States, senior U.S. officials familiar with the case said.

In the tape, an Afghan grain dealer is seen being tortured by a member of the royal family of Abu Dhabi, one of the UAE's seven emirates.

The senior U.S. officials said the administration has held off on the ratification process because it believes sensitivities over the story can hurt its passage. The tape emerged in a federal civil lawsuit filed in Houston, Texas, by Bassam Nabulsi, a U.S. citizen, against Sheikh Issa bin Zayed al Nahyan. Former business partners, the men had a falling out, in part over the tape. In a statement to CNN, the sheikh's U.S. attorney said Nabulsi is using the videotape to influence the court over a business dispute.

The civil nuclear agreement was signed in January between the United Arab Emirates and the Bush administration, but after the new administration took office, the deal had to be recertified. Secretary of State Hillary Clinton recently signed the document and sent it to President Obama for his signature. It should have reached Capitol Hill by now, the senior U.S. officials say, but Obama hasn't yet signed it. And officials say it deliberately has not yet been sent to Congress for ratification.

"It's being temporarily held up because of that tape," one senior official said.

The senior U.S. officials say they are worried that lawmakers critical of the deal could use the videotape to undermine the agreement. The officials say lawmakers could argue the United States should not have such nuclear cooperation with a country where the rule of law is not respected and human rights violations are tolerated. Nabulsi's lawyer, Anthony Buzbee, told CNN he sent letters and excerpts of the tape to lawmakers.

The case reflects the complexities of U.S. foreign policy and may represent a test of the Obama administration's commitment to human rights as it marks its 100th day.

The State Department had little to say publicly on the torture tape incident, but its 2008 human rights report about the United Arab Emirates refers to "reports that a royal family member tortured a foreign national who had allegedly overcharged him in a grain deal." When asked about the case, Acting State Department spokesman Robert Wood said only, "We urge all governments to fully investigate allegations of criminal acts."

On Wednesday, an Abu Dhabi government agency issued a statement deploring the video and promising a full investigation.

"The Government of Abu Dhabi unequivocally condemns the actions depicted on the video and will conduct a comprehensive review of the matter immediately," said the statement issued by the Judicial Department's Human Rights Office, which promised to make its findings public.

U.S. Rep. James McGovern -- the Massachusetts Democrat who co-chairs the congressional Human Rights Commission -- wrote Secretary Clinton expressing "outrage and concern" over the tape and asked her to take a "lead role" in investigating the case, including whether a Department of Homeland Security official working out of the U.S. Embassy in Abu Dhabi failed to bring the case to the attention higher ranking U.S. officials for action after being shown the tape by Nabulsi.

McGovern asked Clinton to "place a temporary hold on further U.S. expenditures of funds, training, sales or transfers of equipment or technology, including nuclear until a full review of this matter and its policy implications

can be completed." He also asked that the United States deny any visa for travel to the United States by Sheikh Issa or his immediate family, including his 18 brothers, several of whom are ruling members of the UAE government.

UAE Crown Prince Mohammed bin Zayed Al Nahyan, a half-brother of Sheikh Issa, is expected to visit Washington sometime next month.

In a phone interview with CNN, McGovern said the tape "should give everyone pause before moving forward with a nuclear cooperation deal until there is just resolution to this."

"How do you justify not only normal relations but providing military technology and a nuclear deal when impunity seems to be the way they do business," he said. "I think we have an obligation to say that we want to step back a bit and look at this a little more closely. If we have any credibility we need to stand firm even when it may be in terms of our geopolitical or strategic interest. This is brutal torture."

Under the "1-2-3 deal," similar to one the United States signed last year with India, Washington would share nuclear technology, expertise and fuel. In exchange, the UAE commits to abide by the Nuclear Non-proliferation Treaty and the International Atomic Energy Agency safeguards.

The small oil-rich Gulf nation promises not to enrich uranium or to reprocess spent nuclear fuel to extract plutonium, which can be used to make nuclear bombs.

The deal is part of a major UAE investment in nuclear, and it has already signed deals to build several nuclear power plants.

The United States already has similar nuclear cooperation agreements with Egypt and Morocco, and U.S. officials said Washington is working on similar pacts with Saudi Arabia, Bahrain and Jordan.

When the Bush administration signed the deal in January, it stressed the UAE's role in global nonproliferation initiatives, including a donation of \$10 million to establish an International Atomic Energy Agency international fuel bank.

The United States has praised the UAE's development of nuclear energy, a stark contrast to criticism of Iran, which is suspected of attempting to enrich uranium for a nuclear bomb.

Congressional critics fear the deal could spark an arms race and proliferation in the region, and the UAE's ties to Iran also have caused concern.

Iran is among the UAE's largest trading partners. In the past, the port city of Dubai, one of the UAE's seven emirates, has been used as a transit point for sensitive technology bound for Iran.

Dubai was also one of the major hubs for the nuclear trafficking network run by Pakistani nuclear scientist Abdul Qadeer Khan, who admitted to spreading nuclear technology to Iran, North Korea and Libya up until the year 2000. He was eventually pardoned by the Pakistani government.

Such ties contributed to stiff opposition in Congress to the failed deal for Dubai Ports World to manage U.S. ports.

Officials said they expect the deal to be sent up to the Hill for ratification within the next few weeks, given that there has been little blowback from the publication of the tape, except for McGovern's letter to Clinton.

"It will be sent very soon," one official said.

UAE Ambassador to the U.S. Yousef Al Otaiba told CNN his government always expected the deal to be sent to the Senate in early May, regardless of the controversy surrounding the tape.

"As far as we are concerned, the deal is on track and this has not affected the timing," he said.

But McGovern told CNN he plans to hold hearings on the matter, including looking into allegations that more tapes depicting Sheikh Issa torturing victims exist.

"This will not blow over," he said. "This is going to have to be addressed in some way, but it is not going to be addressed by saying let's wait a few months and see if it goes away."

<http://edition.cnn.com/2009/WORLD/meast/04/29/uae.nuke.deal/>

[\(Return to Articles and Documents List\)](#)

30 April 2009

US Can Make Sure Pak Nukes are Secure: Obama

Chidanand Rajghatta, TNN

WASHINGTON: US President Barack Obama on Wednesday said Washington "can make sure that Pakistan's nuclear arsenal is secure," even as he expressed grave concern over the deteriorating situation in the militancy-stricken country.

At a White House press conference to mark his first 100 days in office, Obama expressed confidence about US control over Pakistan's nuclear weapons, perhaps through military-to-military cooperation, in the face of extremist advances in the country. In the process, he also hinted that Washington had contingency plans to handle the situation if it went out of Islamabad's hands.

Asked if he could reassure the American people that, if necessary, America could secure Pakistan's nuclear arsenal and keep it from getting into the Taliban's hands, Obama replied: "I'm confident that we can make sure that Pakistan's nuclear arsenal is secure, primarily, initially, because the Pakistani army, I think, recognizes the hazards of those weapons falling into the wrong hands."

The carefully calibrated reply referring to primary security appeared to suggest the US has secondary back-up plans in the event of any exigencies, something the intelligence analysts' community has long considered inevitable.

When the reporter followed up to seek a more precise answer, asking if in the worst case scenario, the US military could secure the nuclear weapons, Obama responded crisply: "I'm not going to engage in hypotheticals of that sort. I feel confident that that nuclear arsenal will remain out of militant hands. Okay?"

The exchange was punctuated by a suo motu expression of concern about the situation in Pakistan by the US President, not because it was about to be overrun by Taliban, he said, but because the civilian government was very fragile and was not delivering basic services and governance, which was providing space for extremists.

It was a surprisingly blunt vote of no-confidence in a civilian government whose leader is about to embark on a visit to Washington next week. There has been speculation in some quarters that Washington is not averse to another military takeover if the civilian government does not assert itself over the extremists.

Obama also referred to what has now become a mantra for his administration: Pakistan should stop worrying about the non-existent military threat from India and tackle its own home-grown extremism.

"On the military side, you're starting to see some recognition just in the last few days that the obsession with India as the mortal threat to Pakistan has been misguided, and that their biggest threat right now comes internally," Obama said, adding, "we want to continue to encourage Pakistan to move in that direction, and we will provide them all the cooperation that we can."

The President seemed to be referring to the reported movement of some 6000 Pakistani troops from the border with India to its western areas recently, even as he made the case for a large civilian and military aid package for Pakistan that Congress is going to take up in the next few days, ahead of the visit to Washington DC next weekend by President Asif Ali Zardari. The 6000 troops were moved to the Indian border in the aftermath of the Mumbai massacre, so essentially the Pakistan military has returned to the pre-Mumbai configuration.

There is strong pressure on Pakistan from Washington to deploy regular troops rather than its constabulary or paramilitary in the battles against extremists, but Islamabad is said to be desisting, holding out for greater military aid and equipment to carry out the task.

There is considerable tension between the two sides on this issue, and a perceptible lack of trust in Washington about Pakistan's claims that it is routing the extremists and re-established control in the territories it has lost to them. The suggestion here is that Pakistan is shadow boxing to ensure the U.S aid package gets through and its military is yet to get rid of its India fixation.

At a separate briefing earlier in the day, a state department spokesman said the US was "happy to see Pakistan taking these types of steps. They need to continue to confront these violent extremists."

Pakistan's histrionics vis-à-vis India was also the subject of a scathing review by vice-president Joe Biden at a separate engagement in Houston where he was quoted as saying Islamabad needs a "cultural change" to view that India is not its enemy.

On one issue however, Obama was unrelenting vis-à-vis Pakistan: The Predator strikes.

"We want to respect their sovereignty, but we also recognize that we have huge strategic interests, huge national security interests, in making sure that Pakistan is stable and that you don't end up having a nuclear-armed militant state," he said, without explicitly referring to the Drone issue that has caused much bad blood between the two countries.

While almost all questions at the 100-day press conference pertained to domestic issues, Pakistan was about the only foreign policy subject, not counting the swine flu issue concerning Mexico. And the Obama message to Pakistan was again unmistakable: Tough love.

<http://timesofindia.indiatimes.com/US-can-make-sure-Pak-nukes-are-secure-Obama/articleshow/4467088.cms>

[\(Return to Articles and Documents List\)](#)

Indian Express
April 30, 2009

Safety of Pak Nukes: Obama does not Rule out Intervention

Agencies

Washington: Leaving open the option of US intervention, President Barack Obama on Thursday said his country had "huge" strategic and security interests in making sure that Pakistan is stable and its nuclear weapons do not fall into militant hands.

"We want to respect their sovereignty, but we also recognise that we have huge strategic interests – huge national security interests – in making sure that Pakistan is stable and that you don't end up having a nuclear-armed militant state," Obama said in a prime-time news conference marking the 100-day of his presidency.

But Obama said he was confident that Pakistan's nuclear arsenal was secure, "because the Pakistani army, I think, recognises the hazards of those weapons falling into the wrong hands."

When pressed whether the United States would intervene if Pakistan's nuclear arsenal were under threat, Obama, speaking at his third White House press conference since assuming office on January 20, said he would not respond to a "hypothetical question."

"I am gravely concerned about the situation in Pakistan, not because I think that they're immediately going to be overrun and the Taliban would take over in Pakistan," Obama said.

"I'm more concerned that the civilian government there right now is very fragile," Obama said.

"I'm more concerned that the civilian government there right now is very fragile and don't seem to have the capacity to deliver basic services: schools, health care, rule of law, a judicial system that works for the majority of the people."

At the same time, Obama said that the civilian government of President Asif Ali Zardari, who is to visit Washington next week, was unable to offer basic services that would ensure people's support and loyalty.

He also said that Pakistan's military had just recently started to change its traditional animosity towards India.

"You're starting to see some recognition just in the last few days that the obsession with India as the mortal threat to Pakistan has been misguided and that their biggest threat right now comes internally," Obama said.

Pakistan, the Muslim world's only nuclear weapons state, has been critical of US infringement on its sovereignty, particularly of regular drone attacks on high-value terror targets in its restive tribal region.

<http://www.indianexpress.com/news/safety-of-pak-nukes-obama-does-not-rule-out-intervention/452986/>

[\(Return to Articles and Documents List\)](#)

China View
28 April 2009

China Rejects Japan's Accusation over Its Nuclear Policy

BEIJING, April 28 (Xinhua) -- China rejected Japan's accusation over withholding information about its nuclear policy here on Tuesday, saying the accusation was groundless.

Jiang Yu, spokeswoman of Chinese Foreign Ministry, told a regular press conference that China had all along advocated and positively supported the comprehensive ban on nuclear weapons and complete nuclear disarmament.

Japanese Foreign Minister Hirofumi Nakasone accused China of withholding information about its nuclear weapons while delivering a speech in Tokyo on Monday.

The speech, entitled "Conditions towards Zero -- 11 Benchmarks for Global Nuclear Disarmament", came in supportive response to the remarks made on April 5 by U.S. President Barack Obama, who advocated a world without nuclear weapons and declared Washington's "moral responsibility to act" to that end.

"China supports the process of international nuclear disarmament, and has made unremitting efforts for it," said Jiang.

Jiang also stressed that China's nuclear policy was clear and transparent. "Japan's accusation is completely groundless."

http://news.xinhuanet.com/english/2009-04/28/content_11274603.htm

[\(Return to Articles and Documents List\)](#)

Straits Times - Singapore

28 April 2009

China: Open about Nuclear

BEIJING - CHINA said on Tuesday that it is completely transparent about its nuclear arsenal and dismissed a call by Japan for more information ahead of a visit by the Japanese prime minister.

China's Foreign Ministry spokeswoman Jiang Yu told reporters China supports international nuclear disarmament efforts and had made 'unremitting efforts' for a ban of nuclear weapons.

'China's nuclear strategy and policies are very clear and completely transparent. The accusations of the Japanese side in this regard are completely groundless,' Jiang told a news conference.

China's annual double-digit percentage increases in military spending have rattled its Asian neighbors, and Washington has warned Beijing's failure to clearly declare its intentions could prompt further unease.

Japan's Foreign Minister Hirofumi Nakasone criticized Beijing on Monday for withholding information about its nuclear weapons and urged greater transparency.

'China continues to modernize its nuclear arsenals but has not undertaken any nuclear arms reductions,' he said at a Tokyo hotel to outline a Japanese initiative for global nuclear disarmament.

'Nor does the country disclose any information on its nuclear arsenals.' China exploded its first nuclear weapon in 1964, but the exact size of its arsenal is unknown.

Japan, the only country to suffer atomic attacks at the end of World War II, supports President Barack Obama's speech at the beginning of April mapping out his vision to achieve a world without atomic weapons, Nakasone said.

Beijing says its nuclear weapons development is for defense only.

Japanese Prime Minister Taro Aso arrives in Beijing on Wednesday for a two-day official visit to focus on strengthening political trust and cooperating to overcome the financial crisis, spokeswoman Jiang said. -- AP

http://www.straitstimes.com/Breaking%2BNews/Asia/Story/STIStory_369684.html

[\(Return to Articles and Documents List\)](#)

Yonhap News

28 April 2009

N. Korea Raps Japan over Stalled Nuclear Talks

By Kim Hyun

SEOUL, April 28 (Yonhap) -- North Korea blasted Japan on Tuesday for passing the blame over stalled nuclear disarmament talks, insisting Tokyo is responsible for the deadlock by not fulfilling its obligations.

The criticism came in response to Japan's Chief Cabinet Secretary Takeo Kawamura, who a day earlier denounced Pyongyang's reprocessing of spent nuclear fuel rods as "not constructive" and urged the country to return to the six-party talks.

"Kawamura's absurd speech, the same as a dog's barking in the moonlight, is not even worth discussing," North Korea's Cabinet newspaper Minju Joson said in a commentary.

"The Japanese reactionary forces... are pointing their finger at us and seriously provoking the Korean military and the people," the paper said, warning, "This is not empty talk."

"But now that he is taking issue with the Sept. 19 joint statement and passing the responsibility for wrecking the six-party talks to us, we must bring up the matter," it said. The joint statement refers to a landmark agreement the two Koreas, the United States, China, Japan and Russia reached in 2005 to resolve the dispute over North Korea's nuclear weapons program.

The nuclear talks have been in limbo since late last year due to disputes over how to verify Pyongyang's past nuclear activity. Tension spiked markedly after North Korea's rocket launch on April 5, which led to a series of punitive reactions from the international community.

The U.N. Security Council adopted a presidential statement condemning the launch, prompting Pyongyang to withdraw from the six-party talks in protest. Last week, the Security Council's sanctions committee froze foreign assets of three North Korean firms suspected of aiding the country's nuclear and missile programs. In response Pyongyang swiftly announced it has begun reprocessing spent nuclear fuel rods to extract plutonium, used to make nuclear bombs.

Kawamura said in a press conference that Japan will fulfill U.N. sanctions and closely work with the U.S. to push the nuclear talks forward.

North Korea accused the Japanese government of politicizing its rocket launch to fend off internal criticism. Japan also failed to provide its share of energy aid promised to Pyongyang under a six-party deal and tried to link an "irrelevant" abduction issue to the nuclear negotiations, the newspaper said.

Under a 2007 deal, Pyongyang was promised 1 million tons of energy aid from the five other nations, and about three quarters of it has been delivered so far. Japan refuses to provide its share of the energy until North Korea's past abduction of its citizens are accounted for.

North Korea's party newspaper, the Rodong Sinmun, also lashed out at South Korea's foreign minister over his stern messages aimed at Pyongyang. The paper accused Yu Myung-hwan of trying to "maliciously harm his brethren, riding on the back of foreign forces," by pushing for Seoul's participation in a U.S.-led security campaign, the Proliferation Security Initiative, and interfering with inter-Korean issues.

<http://english.yonhapnews.co.kr/northkorea/2009/04/28/68/0401000000AEN20090428003600315F.HTML>

[\(Return to Articles and Documents List\)](#)

RIA Novosti

29 April 2009

North Korea Threatens New Nuclear, Ballistic Missile Tests

MOSCOW, April 29 (RIA Novosti) - North Korea said on Wednesday it would conduct further nuclear tests and rocket launches if the UN Security Council did not apologize for its recent criticism of Pyongyang, South Korea's Yonhap said.

The reclusive communist regime announced it was resuming work at its nuclear facilities that produce weapons-grade plutonium and withdrawing from six-nation talks after the UN Security Council condemned a rocket launch on April 5, which Pyongyang said was carrying a communications satellite.

Yonhap also cited North Korea's Foreign Ministry as saying that Pyongyang had decided to build a nuclear power plant with light-water reactors and develop its own technology to produce fuel for these reactors.

Pyongyang's announcements follow U.N. Security Council's criticism over a recent North Korean rocket launch and the approval of new sanctions against three major North Korean companies - Korea Mining Development Trading Corp., Korea Ryongbong General Corp., and the Tanchon Commercial Bank, which are suspected of involvement in ballistic missile transactions.

The North has also expelled IAEA and U.S. nuclear inspectors involved in monitoring the country's disablement progress.

The six-nation talks, involving North and South Korea, Russia, Japan, China and the United States, were launched in 2003 after Pyongyang withdrew from the Nuclear Nonproliferation Treaty.

Under deals reached in 2007, the North began disabling a nuclear reactor and other facilities at Yongbyon under U.S. supervision in exchange for economic aid and political incentives.

However, in December, the latest round of six-party talks resulted in deadlock over a U.S. demand that nuclear inspectors be allowed to take samples out of the country from North Korean facilities for further analysis.

Russian Foreign Minister Sergei Lavrov, who recently visited Pyongyang, said on April 24 that North Korea had no plans to return to six-nation talks, and expressed hope that the situation around North Korea's nuclear and missile programs would not be used as a pretext for the proliferation of nuclear weapons in the region.

<http://en.rian.ru/world/20090429/121366633.html>

[\(Return to Articles and Documents List\)](#)

Yonhap News
29 April 2009

N. Korea Reaffirms Boycott of Nuclear Talks

By Lee Chi-dong

SEOUL, April 29 (Yonhap) -- North Korea will make good on its pledge to quit the multilateral disarmament talks and bolster its nuclear deterrence despite sanctions from the United Nations, the country's leading newspaper said Wednesday.

"We state again that our country will no longer enter into the six-way talks and will strengthen nuclear deterrence power in every way," the Rodong Sinmun, published by the North's powerful Workers' Party, said in a commentary carried by the country's official news agency. ""Under current situations, we are not interested in the six-way talks any more."

The commentary said that the international community's punishment of North Korea's rocket launch reminded it of the importance of beefing up its self-defense measures.

It said the six-way talks lost all reason to exist after the U.N. Security Council issued a presidential statement condemning the April 5 rocket launch. It called the U.N. move a violation of the spirit of a historic aid-for-denuclearization deal signed on Sept. 19 2005 that calls for respecting the sovereignty of each nation. Under the six-way agreement, North Korea promised to abandon its nuclear program in return for economic and political incentives.

"In the unjust and unstable world today, whose international law, relations, and order are swayed by power, we can defend our sovereignty and show dignity and prowess only through defensive nuclear deterrence capability," it added, accusing the U.S., Japan, and other nations of attempting to draw concessions from Pyongyang through increased pressure and sanctions.

Last week, a U.N. Security Council committee blacklisted three North Korean firms suspected of being involved in Pyongyang's development and trade of missiles and weapons of mass destruction.

It was the first concrete follow-up measure to the council's decision to reactivate the 2006 resolution against the North's missile and nuclear tests.

North Korea, infuriated by the document, announced that it will never return to the six-way talks also involving the U.S., South Korea, China, Russia, and Japan. It also said that it has resumed reprocessing plutonium at its main nuclear facilities in Yongbyon.

South Korean officials acknowledge difficulties in finding a breakthrough in the stalemate but pin their hopes on the role of the U.S. and China.

They said Stephen Bosworth, Washington's point man on Pyongyang, is expected to make a tour of Northeast Asia next month to discuss ways to revive the denuclearization process.

"We have information that he is pushing for a trip to the region in May, but detailed schedules have yet to be decided," a South Korean foreign ministry official said on condition of anonymity.

He refused to predict whether Bosworth will visit Pyongyang. North Korea rejected Bosworth's informal proposal to travel there during his Asia swing in March. He was carrying a letter from President Barack Obama to the North's leader Kim Jong-il at that time but did not get a chance to deliver it.

Citing unidentified sources in Washington, the Hankook Ilbo, a South Korean daily, reported Wednesday the U.S. may send former President Jimmy Carter or New Mexico Governor Bill Richardson to North Korea in an effort to win the release of two American journalists detained there for more than a month.

Pyongyang said last week that the female journalists caught during a news reporting trip along the border between North Korea and China will be put to trial, accusing them of illegally trespassing across the border and engaging in "hostile acts."

"I think it is still early to talk about a U.S. envoy because the U.S. is likely to wait for the results of the trial," the ministry official said.

In 1996, Richardson, then a congressman, flew to Pyongyang and successfully negotiated the release of an American citizen, Evan Hunziker, who had been held for three months on suspicion of spying after swimming across the Yalu River that runs along the North Korea and China border.

<http://english.yonhapnews.co.kr/northkorea/2009/04/29/41/0401000000AEN20090429005700315F.HTML>

[\(Return to Articles and Documents List\)](#)

New York Times

April 30, 2009

N. Korea Issues Threat on Uranium

By CHOE SANG-HUN

SEOUL, South Korea — North Korea said Wednesday that it would start a uranium enrichment program, declaring for the first time that it intended to pursue a second project unless the United Nations lifted sanctions.

Calling the United Nations Security Council "a tool for the U.S. highhanded and arbitrary practices," North Korea also threatened to conduct nuclear and intercontinental ballistic missile tests.

It would take North Korea months to prepare a nuclear or ballistic missile test, and some Western intelligence agencies suspect that it has already been pursuing a covert uranium-based nuclear program in parallel to its known plutonium-based program. New nuclear tests would use up some of North Korea's fissile material, but give it more information to improve its technology, as would new missile tests.

By making public threats, the North used a familiar tactic to raise the stakes in its standoff with Washington. Analysts say the country needs outside aid to feed its own people and outside enemies to justify its harsh rule. Since the collapse of the Soviet bloc, when North Korea lost most of its trade partners and aid providers, the impoverished country has used threats as a survival tactic. (When the United States and South Korea provide the North with aid, the government internally tells its people that the "enemies come groveling with tributes.")

North Korea's nuclear program remains its main, and perhaps only, attention-gathering tool and bargaining chip, and it has repeatedly wrested more aid from its threats, and even new bouts of engagement with Washington.

The North's first nuclear test in 2006 was considered something of a failure by the United States and South Korea. And a North Korean ballistic missile launched in 2006 blew up 40 seconds after blastoff and, contrary to North Korean claims, another rocket launched in early April failed to put a satellite into orbit, American officials said.

On April 13, the Security Council issued a unanimous statement denouncing the North's rocket launching as a violation of a resolution after the North's first nuclear test in 2006 that banned the country from nuclear and ballistic missile tests. The Council called for tightening sanctions, a move that the North on Wednesday said was tantamount to "a declaration of war."

A Foreign Ministry spokesman told the state-run news agency, KCNA, that the country would "take additional self-defensive measures" unless the Security Council apologized immediately, specifying "nuclear tests and test-firings of intercontinental ballistic missiles."

North Korea also "will make a decision to build a light-water reactor power plant and start the technological development for ensuring self-production of nuclear fuel as its first process without delay," the spokesman said. Such fuel would be uranium-based. Engineers use the same fuel-making technology to produce highly enriched uranium for nuclear bombs.

North Korea reportedly has told United States officials that it has extracted enough plutonium for several bombs by reprocessing spent nuclear fuel. But it has never confirmed that it has been pursuing a clandestine uranium-enrichment program that would provide an alternative means of bomb-making.

On Wednesday, Fred Lash, a State Department spokesman, defended the Security Council's action as "balanced and appropriate."

"We certainly call on North Korea, as we have in the past, to uphold its commitments" under two documents, he said: a Sept. 19, 2005, joint statement of six-party talks on North Korea, and a 2006 Security Council resolution imposing sanctions.

"We remain committed to achieving the verifiable denuclearization of the Korean Peninsula, hopefully through the six-party talks," he said. "We urge them, as we always do, to return to the table."

The North insisted that its April launching, conducted after it ignored repeated offers of dialogue from Washington, was solely to put a communications satellite into orbit. But Washington maintained that the launching was a disguise for testing ballistic missile technology.

Over the weekend, Secretary of State Hillary Rodham Clinton said Washington would not be "blackmailed" by the North. The United States and its allies will "tighten the band around North Korea," she said.

Washington's approach appears to be based partly on a belief that the North's recent moves were meant more for domestic purposes than to gain leverage internationally. Since his reported stroke in August, North Korea's leader, Kim Jong-il, seems to have shifted his priority to demonstrating leadership and securing a stable transfer of power to one of his three sons. And the best way to do so, experts say, is to highlight the one achievement Mr. Kim can boast of: his nuclear and missile programs.

Washington's current stand on North Korea has raised some concern in Seoul. After recent policy discussions in Washington, Moon Chung-in, a North Korea expert at Yonsei University in Seoul, described the American attitude as "just like the first-term Bush administration."

Shin Nakyun, a South Korean lawmaker, who also attended the discussions, said: "Although they said they keep their door open for North Korea, I felt they were turning uniformly hard-line. They said there will be no carrots for the North."

The Bush administration reversed its refusal to engage the North after the North conducted its first nuclear test in 2006. Washington offered a string of concessions but was disappointed when North Korea did not acknowledge the suspected uranium-enrichment program or helping Syria on nuclear issues.

<http://www.nytimes.com/2009/04/30/world/asia/30korea.html?em>

[\(Return to Articles and Documents List\)](#)

Philadelphia Inquirer
April 29, 2009

Extremists said to be Eyeing Somalia as New Base

By Lolita C. Baldor, Associated Press

WASHINGTON -- There is growing evidence that battle-hardened extremists are filtering out of safe havens along the Pakistan-Afghanistan border and into East Africa, bringing sophisticated terror tactics that include suicide attacks.

The shift, according to U.S. military and counterterrorism officials, fuels concern that Somalia, in particular, could become the next Afghanistan - a sanctuary where al-Qaeda-linked groups could train and plan attacks against the West.

So far, officials say, the number of foreign fighters who have moved from southwest Asia and the Afghanistan-Pakistan border region to the Horn of Africa is small, perhaps two to three dozen.

But a similarly small cell of plotters was responsible for the devastating 1998 bombings of U.S. embassies in Kenya and Tanzania.

The cluster of extremists now believed to be operating inside East Africa could pass on sophisticated training and attack techniques gleaned from seven years at war against the United States and its allies in Iraq and Afghanistan, U.S. officials said.

"There is a level of activity that is troubling, disturbing," said Gen. William "Kip" Ward, head of U.S. Africa Command. "When you have these vast spaces that are just not governed, it provides a haven for support activities, for training to occur."

Ward added that U.S. officials already were seeing extremist factions in East Africa sharing information and techniques.

Several military and counterterrorism officials who spoke on condition of anonymity to discuss sensitive intelligence matters cautioned that the movements of the al-Qaeda extremists did not suggest they were abandoning the ungoverned Pakistan border region as a safe haven.

Instead, the officials view the shift more as an expansion of al-Qaeda's influence.

Last month, Osama bin Laden - who spent five years in Sudan before he was expelled in 1996 and relocated to Afghanistan - made it clear in an audiotape that al-Qaeda has set its sights on Somalia, an impoverished, lawless country in the Horn of Africa.

In the 11-minute tape released to Internet sites, bin Laden is heard urging Somalis to overthrow their new moderate Islamist president and to support their jihadist "brothers" in Afghanistan, Pakistan, Iraq, and the Palestinian territories.

Officials said that in recent years they have seen signs that terror techniques bearing al-Qaeda's signature are gaining ground in East Africa. The harbingers include coordinated suicide bombings in Somalia in October.

In the past, officials said, suicide attacks had tended to be frowned on by African Muslims.

But on Oct. 29, 2008, suicide bombers killed more than 20 people in five attacks in Somalia, targeting a U.N. compound, the Ethiopian consulate, the presidential palace in Somaliland's capital, and two intelligence facilities in Puntland.

The incident also marked the first time that a U.S. citizen - a young Somali man from Minneapolis - carried out a suicide bombing.

The foreign fighters moving into East Africa complicate an already-rising crescendo of threats in the region. Those threats have come from the Somalia-based al-Shabab extremist Islamic faction and from al-Qaeda in East Africa, a small, hard-core group also known by the acronym EEAQ.

While not yet considered an al-Qaeda franchise, EEAQ has connections to the top terror leaders and was implicated in the August 1998 embassy bombings in Tanzania and Kenya that killed 225 people.

Al-Qaeda has the skills while al-Shabab has the manpower, said one senior military official familiar with the region. The scenario could become even more worrisome, the officials said, if the foreign fighters transplant their skills at bomb-making and insurgency tactics to the training camps in East Africa.

http://www.philly.com/inquirer/world_us/20090429_Extremists_said_to_be_eyeing_Somalia_as_new_base.html

[\(Return to Articles and Documents List\)](#)

New York Daily News
April 30th 2009

Al Qaeda No. 2 Ayman al-Zawahiri calls the Shots, says State Department

BY James Gordon Meek
DAILY NEWS WASHINGTON BUREAU

WASHINGTON - Al Qaeda's No. 2 thug has "emerged" as its operational leader after seven years on the run with the same \$25 million bounty on his head as Osama Bin Laden.

Despite years of Bush administration claims that Ayman al-Zawahiri - an Egyptian doctor turned Bin Laden deputy - was on the lam with his boss and unable to exert control, the opposite is now true, a State Department report said Thursday.

"Al Qaeda has reconstituted some of its pre-9/11 operational capabilities" in Pakistan's tribal safe haven on the Afghan border, replaced lost lieutenants and achieved "the restoration of some central control by its top leadership, in particular Ayman al-Zawahiri," the annual Country Reports on Terrorism said.

"Although Bin Laden remains the group's ideological figurehead, Zawahiri has emerged as Al Qaeda's strategic and operational planner," the report added.

The new assessment wasn't a surprise to terror experts, since Zawahiri put out 12 audio and video messages last year and four this year, including one last week.

"As important as it is to neutralize Al Qaeda's top leaders, you also have to maintain an unblinking focus on disrupting its operations," said Kenneth Wainstein, a top George W. Bush homeland security adviser now with the O'Melveny and Myers law firm.

http://www.nydailynews.com/news/us_world/2009/04/30/2009-04-30_al_qaeda_no_2_calls_the_shots.html

[\(Return to Articles and Documents List\)](#)

Al Jazeera
30 April 2009

US Fears Over al-Qaeda in Pakistan

The al-Qaeda network remains the largest 'terror' threat to the US and is increasingly using Pakistan as its main battleground, a new US report has said.

In the report on what was described as "global terror", the US state department said that attacks in Pakistan more than doubled between 2007 and 2008 and have quadrupled since 2006.

"Pakistan's ... tribal areas provided AQ [Al-Qaeda] many of the benefits it once derived from its base across the border in Afghanistan," the report said on Thursday.

It also warned that the Taliban and al-Qaeda affiliates have increased the "co-ordination, sophistication and frequency" of suicide and other bombings in Pakistan and were challenging the government's authority.

And it said that efforts to combat the Taliban in Afghanistan in particular needed a global approach.

"The international community's assistance to the Afghan government to build counterinsurgency capabilities, ensure legitimate and effective governance, and counter the surge in narcotics cultivation is essential to the effort to defeat the Taliban and other insurgent groups and criminal gangs," it said.

'Gravely concerned'

The White House has made Pakistan and neighbouring Afghanistan a central plank of its foreign policy, with Barack Obama, the US president, to send 21,000 more US troops to Afghanistan and asking congress for aid to assist the Pakistani army.

Obama has also put pressure on Pakistan to produce results in its efforts to combat the Taliban and al-Qaeda, saying in a news conference on Thursday he remained "gravely concerned" about the security situation in the country.

The US has become increasingly concerned about the stability of nuclear-armed Pakistan, a US ally seen as vital to stabilising Afghanistan, as the Taliban have advanced from their Swat valley stronghold to within 100km of Pakistan's capital.

Obama's comments came after Pakistani troops were reported to have regained control of the main town in Buner district from the Taliban in the country's North West Frontier Province.

In total, attacks in South Asia, including Afghanistan and Pakistan, accounted for 35 per cent of the 11,770 attacks that took place worldwide in 2008, the report said.

However, the total number of terror attacks fell from 14,506 in 2007 and the number of deaths also dropped to 15,765 from 22,508.

The report said the threat from al-Qaeda in Iraq had diminished following defections and a loss of funding and control in key areas and "improved capabilities" of Iraqi forces and Sunni tribes' so-called Awakening Councils.

Iran was also strongly criticised as the "most significant state sponsor of terrorism", with the report saying Iran continued to employ "terrorism to advance its key national security and foreign policy interests".

<http://english.aljazeera.net/news/americas/2009/04/2009430181416309946.html>

[\(Return to Articles and Documents List\)](#)

New York Times

April 28, 2009

U.S. Steps Up Effort on Digital Defenses

By David E. Sanger, John Markoff and Thom Shanker

When American forces in Iraq wanted to lure members of Al Qaeda into a trap, they hacked into one of the group's computers and altered information that drove them into American gun sights.

When President George W. Bush ordered new ways to slow Iran's progress toward a nuclear bomb last year, he approved a plan for an experimental covert program — its results still unclear — to bore into their computers and undermine the project.

And the Pentagon has commissioned military contractors to develop a highly classified replica of the Internet of the future. The goal is to simulate what it would take for adversaries to shut down the country's power stations, telecommunications and aviation systems, or freeze the financial markets — in an effort to build better defenses against such attacks, as well as a new generation of online weapons.

Just as the invention of the atomic bomb changed warfare and deterrence 64 years ago, a new international race has begun to develop cyberweapons and systems to protect against them.

Thousands of daily attacks on federal and private computer systems in the United States — many from China and Russia, some malicious and some testing chinks in the patchwork of American firewalls — have prompted the Obama administration to review American strategy.

President Obama is expected to propose a far larger defensive effort in coming days, including an expansion of the \$17 billion, five-year program that Congress approved last year, the appointment of a White House official to coordinate the effort, and an end to a running bureaucratic battle over who is responsible for defending against cyberattacks.

But Mr. Obama is expected to say little or nothing about the nation's offensive capabilities, on which the military and the nation's intelligence agencies have been spending billions. In interviews over the past several months, a range of military and intelligence officials, as well as outside experts, have described a huge increase in the sophistication of American cyberwarfare capabilities.

Because so many aspects of the American effort to develop cyberweapons and define their proper use remain classified, many of those officials declined to speak on the record. The White House declined several requests for interviews or to say whether Mr. Obama as a matter of policy supports or opposes the use of American cyberweapons.

The most exotic innovations under consideration would enable a Pentagon programmer to surreptitiously enter a computer server in Russia or China, for example, and destroy a "botnet" — a potentially destructive program that

commandeers infected machines into a vast network that can be clandestinely controlled — before it could be unleashed in the United States.

Or American intelligence agencies could activate malicious code that is secretly embedded on computer chips when they are manufactured, enabling the United States to take command of an enemy's computers by remote control over the Internet. That, of course, is exactly the kind of attack officials fear could be launched on American targets, often through Chinese-made chips or computer servers.

So far, however, there are no broad authorizations for American forces to engage in cyberwar. The invasion of the Qaeda computer in Iraq several years ago and the covert activity in Iran were each individually authorized by Mr. Bush. When he issued a set of classified presidential orders in January 2008 to organize and improve America's online defenses, the administration could not agree on how to write the authorization.

A principal architect of that order said the issue had been passed on to the next president, in part because of the complexities of cyberwar operations that, by necessity, would most likely be conducted on both domestic and foreign Internet sites. After the controversy surrounding domestic spying, Mr. Bush's aides concluded, the Bush White House did not have the credibility or the political capital to deal with the subject.

Electronic Vulnerabilities

Cyberwar would not be as lethal as atomic war, of course, nor as visibly dramatic. But when Mike McConnell, the former director of national intelligence, briefed Mr. Bush on the threat in May 2007, he argued that if a single large American bank were successfully attacked "it would have an order-of-magnitude greater impact on the global economy" than the Sept. 11, 2001, attacks. Mr. McConnell, who left office three months ago, warned last year that "the ability to threaten the U.S. money supply is the equivalent of today's nuclear weapon."

The scenarios developed last year for the incoming president by Mr. McConnell and his coordinator for cybersecurity, Melissa Hathaway, went further. They described vulnerabilities including an attack on Wall Street and one intended to bring down the nation's electric power grid. Most were extrapolations of attacks already tried.

Today, Ms. Hathaway is the primary author of White House cyberstrategy and has been traveling the country talking in vague terms about recent, increasingly bold attacks on the computer networks that keep the country running. Government officials will not discuss the details of a recent attack on the air transportation network, other than to say the attack never directly affected air traffic control systems.

Still, the specter of an attack that could blind air traffic controllers and, perhaps, the military's aerospace defense networks haunts military and intelligence officials. (The saving grace of the air traffic control system, officials say, is that it is so old that it is not directly connected to the Internet.)

Studies, with code names like Dark Angel, have focused on whether cellphone towers, emergency-service communications and hospital systems could be brought down, to sow chaos.

But the theoretical has, at times, become real.

"We have seen Chinese network operations inside certain of our electricity grids," said Joel F. Brenner, who oversees counterintelligence operations for Dennis Blair, Mr. McConnell's successor as national intelligence director, speaking at the University of Texas at Austin this month. "Do I worry about those grids, and about air traffic control systems, water supply systems, and so on? You bet I do."

But the broader question — one the administration so far declines to discuss — is whether the best defense against cyberattack is the development of a robust capability to wage cyberwar.

As Mr. Obama's team quickly discovered, the Pentagon and the intelligence agencies both concluded in Mr. Bush's last years in office that it would not be enough to simply build higher firewalls and better virus detectors or to restrict access to the federal government's own computers.

"The fortress model simply will not work for cyber," said one senior military officer who has been deeply engaged in the debate for several years. "Someone will always get in."

That thinking has led to a debate over whether lessons learned in the nuclear age — from the days of "mutually assured destruction" — apply to cyberwar.

But in cyberwar, it is hard to know where to strike back, or even who the attacker might be. Others have argued for borrowing a page from Mr. Bush's pre-emption doctrine by going into foreign computers to destroy malicious software before it is unleashed into the world's digital bloodstream. But that could amount to an act of war, and

many argue it is a losing game, because the United States is more dependent on a constantly running Internet system than many of its potential adversaries, and therefore could suffer more damage in a counterattack.

In a report scheduled to be released Wednesday, the National Research Council will argue that although an offensive cybercapability is an important asset for the United States, the nation is lacking a clear strategy, and secrecy surrounding preparations has hindered national debate, according to several people familiar with the report.

The advent of Internet attacks — especially those suspected of being directed by nations, not hackers — has given rise to a new term inside the Pentagon and the National Security Agency: “hybrid warfare.”

It describes a conflict in which attacks through the Internet can be launched as a warning shot — or to pave the way for a traditional attack.

Early hints of this new kind of warfare emerged in the confrontation between Russia and Estonia in April 2007. Clandestine groups — it was never determined if they had links to the Russian government — commandeered computers around the globe and directed a fire hose of data at Estonia’s banking system and its government Web sites.

The computer screens of Estonians trying to do business with the government online were frozen, if they got anything at all. It was annoying, but by the standards of cyberwar, it was child’s play.

In August 2008, when Russia invaded Georgia, the cyberattacks grew more widespread. Georgians were denied online access to news, cash and air tickets. The Georgian government had to move its Internet activity to servers in Ukraine when its own servers locked up, but the attacks did no permanent damage.

Every few months, it seems, some agency, research group or military contractor runs a war game to assess the United States’ vulnerability. Senior intelligence officials were shocked to discover how easy it was to permanently disable a large power generator. That prompted further studies to determine if attackers could take down a series of generators, bringing whole parts of the country to a halt.

Another war game that the Department of Homeland Security sponsored in March 2008, called Cyber Storm II, envisioned a far larger, coordinated attack against the United States, Britain, Canada, Australia and New Zealand. It studied a disruption of chemical plants, rail lines, oil and gas pipelines and private computer networks. That study and others like it concluded that when attacks go global, the potential economic repercussions increase exponentially.

To prove the point, Mr. McConnell, then the director of national intelligence, spent much of last summer urging senior government officials to examine the Treasury Department’s scramble to contain the effects of the collapse of Bear Stearns. Markets froze, he said, because “what backs up that money is confidence — an accounting system that is reconcilable.” He began studies of what would happen if the system that clears market trades froze.

“We were halfway through the study,” one senior intelligence official said last month, “and the markets froze of their own accord. And we looked at each other and said, ‘Our market collapse has just given every cyberwarrior out there a playbook.’”

Just before Mr. Obama was elected, the Center for Strategic and International Studies, a policy research group in Washington, warned in a report that “America’s failure to protect cyberspace is one of the most urgent national security problems facing the new administration.”

What alarmed the panel was not the capabilities of individual hackers but of nations — China and Russia among them — that experts believe are putting huge resources into the development of cyberweapons. A research company called Team Cymru recently examined “scans” that came across the Internet seeking ways to get inside industrial control systems, and discovered more than 90 percent of them came from computers in China.

Scanning alone does no damage, but it could be the prelude to an attack that scrambles databases or seeks to control computers. But Team Cymru ran into a brick wall as soon as it tried to trace who, exactly, was probing these industrial systems. It could not determine whether military organizations, intelligence agencies, terrorist groups, criminals or inventive teenagers were behind the efforts.

The good news, some government officials argue, is that the Chinese are deterred from doing real damage: Because they hold more than a trillion dollars in United States government debt, they have little interest in freezing up a system they depend on for their own investments.

Then again, some of the scans seemed to originate from 14 other countries, including Taiwan, Russia and, of course, the United States.

Bikini Atoll for an Online Age

Because “cyberwar” contains the word “war,” the Pentagon has argued that it should be the locus of American defensive and offensive strategy — and it is creating the kind of infrastructure that was built around nuclear weapons in the 1940s and ’50s.

Defense Secretary Robert M. Gates is considering proposals to create a Cyber Command — initially as a new headquarters within the Strategic Command, which controls the American nuclear arsenal and assets in space. Right now, the responsibility for computer network security is part of Strategic Command, and military officials there estimate that over the past six months, the government has spent \$100 million responding to probes and attacks on military systems. Air Force officials confirm that a large network of computers at Maxwell Air Force Base in Alabama was temporarily taken off-line within the past eight months when it was put at risk of widespread infection from computer viruses.

But Mr. Gates has concluded that the military’s cyberwarfare effort requires a sharper focus — and thus a specific command. It would build the defenses for military computers and communications systems and — the part the Pentagon is reluctant to discuss — develop and deploy cyberweapons.

In fact, that effort is already under way — it is part of what the National Cyber Range is all about. The range is a replica of the Internet of the future, and it is being built to be attacked. Competing teams of contractors — including BAE Systems, the Applied Physics Laboratory at Johns Hopkins University and Sparta Inc. — are vying to build the Pentagon a system it can use to simulate attacks. The National Security Agency already has a smaller version of a similar system, in Millersville, Md.

In short, the Cyber Range is to the digital age what the Bikini Atoll — the islands the Army vaporized in the 1950s to measure the power of the hydrogen bomb — was to the nuclear age. But once the tests at Bikini Atoll demonstrated to the world the awesome destructive power of the bomb, it became evident to the United States and the Soviet Union — and other nuclear powers — that the risks of a nuclear exchange were simply too high. In the case of cyberattacks, where the results can vary from the annoying to the devastating, there are no such rules.

The Deterrence Conundrum

During the cold war, if a strategic missile had been fired at the United States, screens deep in a mountain in Colorado would have lighted up and American commanders would have some time to decide whether to launch a counterattack. Today, when Pentagon computers are subjected to a barrage, the origin is often a mystery. Absent certainty about the source, it is almost impossible to mount a counterattack.

In the rare case where the preparations for an attack are detected in a foreign computer system, there is continuing debate about whether to embrace the concept of pre-emption, with all of its Bush-era connotations. The questions range from whether an online attack should be mounted on that system to, in an extreme case, blowing those computers up.

Some officials argue that if the United States engaged in such pre-emption — and demonstrated that it was watching the development of hostile cyberweapons — it could begin to deter some attacks. Others believe it will only justify pre-emptive attacks on the United States. “Russia and China have lots of nationalistic hackers,” one senior military officer said. “They seem very, very willing to take action on their own.”

Senior Pentagon and military officials also express deep concern that the laws and understanding of armed conflict have not kept current with the challenges of offensive cyberwarfare.

Over the decades, a number of limits on action have been accepted — if not always practiced. One is the prohibition against assassinating government leaders. Another is avoiding attacks aimed at civilians. Yet in the cyberworld, where the most vulnerable targets are civilian, there are no such rules or understandings. If a military base is attacked, would it be a proportional, legitimate response to bring down the attacker’s power grid if that would also shut down its hospital systems, its air traffic control system or its banking system?

“We don’t have that for cyber yet,” one senior Defense Department official said, “and that’s a little bit dangerous.”

<http://www.nytimes.com/2009/04/28/us/28cyber.html?ref=global-home>

[\(Return to Articles and Documents List\)](#)

National Journal
May 2, 2009

The Cyber Defense Perimeter

By Shane Harris

In response to an unprecedented wave of attacks on the Defense Department's computer networks, and possible theft of information about U.S. weapons systems by foreign governments, the Pentagon has quietly begun sharing classified intelligence about hackers and online threats with the country's biggest defense contractors. The intelligence-sharing program began almost two years ago, after top Pentagon leaders realized that hackers were trying to steal information not just by breaking into government computers but also by going after corporations that contract with the government. These private computers and networks often contain the same sensitive and classified information found in the government's systems.

The new intelligence partnership, which has not been previously reported, is known as the Defense Industrial Base initiative, or "the DIB." The department formally launched the program in September 2007, but it took a year to work out a legal arrangement by which the contractors and the government could confidentially share information. In mid-2008, the effort ramped up after what was described as a hair-raising meeting in a secured facility at the Pentagon in which officials gave temporary security clearances to chief executives from the biggest defense firms and delivered a no-holds-barred briefing on the range of successful cyberattacks launched against the government and their companies. The executives "went in with dark hair and came out with white hair," said James Lewis, a prominent cyber-security expert and a fellow at the Center for Strategic and International Studies, who is familiar with the meeting. "I think that was a shocker for most people."

Weaknesses in corporate defenses can threaten top government secrets. Last month, *The Wall Street Journal* reported that cyber-spies targeted companies helping to build the Joint Strike Fighter and stole design information that could make it easier for adversaries to defend against the airplane. The paper reported that the breaches began as early as 2007 and perhaps continued into 2008, a period that generally coincides with the intelligence-sharing program's start-up.

Since then, Pentagon leaders have met with "the highest levels of all the different companies" in the defense industrial base, a senior Defense official told *National Journal*. Former Deputy Defense Secretary Gordon England "took this as a top priority, and he made sure that we got the highest levels of all the companies aware of the cyber-threat and the whole circumstances around it," said Robert Lentz, the deputy assistant Defense secretary who oversees the intelligence-sharing partnership.

According to a dozen industry and government officials interviewed by *NJ*, the pilot DIB has been running largely unnoticed. It is restricted to companies in the defense sector. But the White House has received a proposal to expand the program to other economic sectors that are at risk of cyberattack, such as the electrical power and financial services industries. In written recommendations to Melissa Hathaway, President Obama's cyber-security adviser, the Intelligence and National Security Alliance, a nonpartisan association of intelligence professionals, called the Pentagon's program a "fledgling effort" that "should be fully supported." The group's former chairman, John Brennan, is Obama's top counter-terrorism and homeland-security adviser.

The Pentagon is working with the Homeland Security Department to broaden the model for other vital infrastructure sectors, Lentz said.

The program has worked out a consistent, if not real-time, process for sharing cyber-intelligence. Every two weeks, the Defense Department briefs the 30 companies participating in the DIB on potential vulnerabilities in computer networks, as well as on specific threats that the government has found in the course of its regular scouting in cyberspace. Experts cull the data from a number of intelligence and military organizations, Lentz said, including the Joint Task Force-Global Network Operations, which is responsible for protecting military computer networks, and the National Security Agency's Threat Operations Center, which monitors global communications networks for threats to defense and intelligence agencies.

The information comes in two forms, Lentz said: an unclassified report that executives can share with the technicians who manage their networks, and a classified report of "contextual information" that the firms can use to protect themselves.

The Defense Department has a compelling interest in protecting the data on its contractors' systems. "This is DOD information that is at risk," Lentz said. The companies may own their networks, but the information traveling on them belongs to the government and is considered a vital national defense asset.

Lentz declined to specify what threats have turned up or what attacks have occurred. But he said that the senior-level attention at the Pentagon was triggered by a notable increase in attacks. "In the past 18 months, we've seen a significant spike in cyber-criminal activity," he said.

A significant portion of that activity appears to be cyber-espionage -- the theft of restricted information through the Internet. Senior defense and intelligence officials have been sounding the alarm for several months about -espionage by computers based in China. They've also singled out organized cyber-crime rings in Russia. In an interview with *NJ* last year, Joel Brenner, the nation's top counter-intelligence official, named both countries as major sources of sophisticated and relentless cyberattacks.

Corporations are reluctant to confirm that they are part of the DIB initiative, and Lentz wouldn't give any names. But sources familiar with the membership say that it includes the top tier of defense contractors, and that smaller companies are joining the group as well. Officials with Raytheon and Northrup Grumman confirmed that their companies are members.

It's not surprising that some contractors want to remain silent. Some executives fear that hackers will only try harder to breach their systems if they know that their networks contain information so valuable that the military and the intelligence community are helping to protect it, according to one industry official who works with the DIB. The program is not classified, but it has created a forum in which contractors feel safe enough to disclose weaknesses in their defenses without fear of inviting attack or drawing public attention.

Historically, corporate leaders have been loathe to share this kind of information with the government for fear of negative press, or because they think it will limit their opportunities to win future business. For nearly a decade, cyber-security experts have warned that the lack of consistent information-flow between government and industry has weakened overall security.

"This is all about trust," Lentz said of the DIB, "and all about a mutual understanding of the consequences of not taking immediate action to find out what's causing a particular event."

The program is not a one-way street. In addition to the regular threat reports that contractors receive from government, they are expected to report any intrusions into their systems within 72 hours of the event, Lentz said. That information goes to a Defense Department cyber-forensics team that specializes in tracing the source of an attack and learning how it was done. "When we determine that someone is trying to attack our networks ... we'll report that very quickly," said Steve Hawkins, vice president of information security solutions at Raytheon. "The government in turn can then provide that information out to the other partners."

Although participants say that the new partnership was not spawned by one particular incident, its birth closely followed a June 2007 attack on Pentagon computer systems that surprised senior officials for its breadth and severity.

As first reported in September 2007 by the *Financial Times*, the Chinese military hacked into a Pentagon computer network three months earlier, in what U.S. officials called "the most successful cyberattack on the U.S. Defense Department." The attack showed an alarming level of sophistication and precision. "China had shown it could disrupt systems at critical times," the newspaper reported.

In September 2007, *Forbes* reported, "the same spies may have been combing through the computer systems of major U.S. defense contractors for more than a year." That same month, the DIB initiative took shape.

The Defense Department was not reacting to an isolated event, Lentz emphasized. "We've been very much concerned about ... the breadth of the cyber-movement in terms of their aggressiveness, their skills sets," he said, calling cyberspace "increasingly volatile"

Lewis of CSIS, who directed a comprehensive cyber-security study for the Obama administration, agreed that the threat was, and is, pervasive and persistent. "It wasn't that we got wacked by a two-by-four; we were getting wacked by a two-by-four every week."

http://www.nationaljournal.com/njmagazine/id_20090502_5834.php

[\(Return to Articles and Documents List\)](#)

RIA Novosti
28 April 2009

Swine Flu Vaccine may be Available in 6 Months - Russian Expert

MOSCOW, April 28 (RIA Novosti) - A Russian expert said on Tuesday a vaccine against swine flu that according to the latest reports has already killed more than 150 people in Mexico could be developed within six months.

The World Health Organization (WHO) has raised its alert level from three to four indicating a significant risk increase and two steps short of a full pandemic.

"A vaccine against swine flu could be developed at best in six months," said Dmitry Lvov, director of the Virology Research Institute at the Russian Academy of Medical Sciences.

WHO officials also said developing a new vaccine could take four to six months.

As of midday Tuesday, swine flu has killed 152 people in Mexico, and over 1,500 others have been hospitalized with symptoms in the Central American country.

Although fifty cases have been reported in the United States, six in Canada, as well as in Spain, Scotland and New Zealand, none of have proved fatal to date.

Lvov assessed the risk of a pandemic spread in the worst scenario as quite high, and warned that swine flu could reach Russia "within hours, or days maximum, anyway within a week."

"It [swine flu] can spread as fast as lightning with the current means of transportation. It is impossible to prevent the virus from entering our country," the Russian expert predicted.

However the director of the State Scientific Virology and Biotechnology Center said on Tuesday the virus currently poses no threat to Russia.

"We do not regard the situation as dangerous in the foreseeable future," Ilya Drozdov said.

The Israeli Health Ministry confirmed on Tuesday the first incidence of swine flu, the country's Kol Israel radio said.

The Israeli victim is a young male who last week returned from Mexico. Another Israeli man, also just back from Mexico, has been hospitalized with flu symptoms.

<http://en.rian.ru/russia/20090428/121348681.html>

[\(Return to Articles and Documents List\)](#)

Daily Telegraph
01 May 2009

Swine Flu: Virus may be on Decline in Mexico

By Tom Leonard in Cancun

Jose Cordova, Mexico's health secretary, said that the number of new cases has flattened out along with the death rate.

He said the next few days would be critical in determining whether the virus was actually on the decline.

Felipe Calderon, the Mexican president, has just ordered a five-day freeze of a large part of his country's economy and urged people to stay at home in order to contain the spread of the flu.

Dr Miguel Angel Lezana, Mexico's most senior epidemiologist, accused the World Health Organisation of being slow to react to an outbreak of atypical pneumonia that grew into the swine flu epidemic.

Dr Lezana, director of the National Epidemiology Centre, said he wanted an investigation into why his staff alerted the Pan American Health Organisation on April 16 about the outbreak in Mexico, but didn't see any action by the WHO, the parent body, until eight days later.

Mexican health officials said they had confirmed 300 swine flu cases and 12 deaths due to the virus among a total of 679 people so far tested.

Less than half of the suspected cases tested have been confirmed as swine flu, and a series of visits to the families of victims also turned up relatively few suspected cases.

"The fact that we have a stabilisation in the daily numbers, even a drop, makes us optimistic," said Mr Cordoba. "Because what we'd expect is geometric or exponential growth. And that hasn't been the situation. So we think we're on the right track."

Dr Keiji Fukada, the WHO's senior flu official, was more cautious. "For things to go up and down in a country is expected. If it didn't do that would be very unusual," he said.

"Hopefully we'll see more of the data of what's going on there. But I expect even in Mexico you will see a mixed picture."

<http://www.telegraph.co.uk/health/swine-flu/5255045/Swine-flu-virus-may-be-on-decline-in-Mexico.html>

[\(Return to Articles and Documents List\)](#)

Washington Post

May 1, 2009

Many States Do Not Meet Readiness Standards

By Kimberly Kindy

Washington Post Staff Writer

More than two dozen states, including Maryland, as well as the District, have not stocked enough of the emergency supplies of antiviral medications considered necessary to treat victims of swine flu should the outbreak become a full-blown crisis, according to federal records.

The medications are part of a national effort to be prepared for a pandemic, and the stockpiling program is being tested for the first time by the rapid spread of the H1N1 strain of the influenza virus. If a health crisis wiped out drug supplies in pharmacies and hospitals, or if families were unable to get to their doctors, local and state officials could quickly distribute stockpiled medications.

The Strategic National Stockpile, created during the Clinton administration a decade ago to provide a federally coordinated response to disasters, maintains a massive collection of antibiotics, vaccines, gas masks and other supplies in a dozen secret locations. The program was expanded in 2004 to include drugs needed in a pandemic and is designed to link with stockpiles kept by state governments, pharmaceutical companies and federal agencies.

But the District, Maryland and 26 other states are 10 million dosages short of the levels that the federal government has determined they should have in their stockpiles for a pandemic. The drugs -- in this case, Tamiflu and Relenza -- would be used to treat the illness, not to prevent it.

Federal agencies, which under the plan are expected to create their own stockpiles, are also falling short. The Postal Service, whose carriers could be needed to deliver medications in a pandemic, has no antiviral medications stocked.

The federal government has met its goal of accumulating 50 million courses of the antiviral medications. Officials said this week that the rollout of those drugs to states has gone smoothly. More than \$6 billion has been invested in efforts to fight a pandemic, and President Obama this week asked for an additional \$1.5 billion from Congress. The Department of Health and Human Services said yesterday that it will purchase an additional 13 million treatment courses.

"We have anticipated this within the United States," Health and Human Services Secretary Kathleen Sebelius said yesterday afternoon. "We are very aggressively addressing cases here, containment here, trying to move rapidly."

Along with the federal doses, the plan called for states together to create a cache of 30 million doses, but they have fallen short of that figure by one-third. Maine, for example, which has three confirmed cases of swine flu, has stockpiled no medications.

The District and Maryland fell short by hundreds of thousands of doses. Virginia is one of 15 states that has stockpiled more doses than called for in the federal guidelines. In the District, health officials stockpiled about 76 percent of the recommended doses, and in Maryland, the figure was about 70 percent, although officials there said they think they will be fully stocked by this fall.

The combined federal-state stockpile would provide enough medication to treat 25 percent of the population. Health officials believe that treatment at such levels would be sufficient to stop a pandemic.

Some states, however, were reluctant to invest in their share for two reasons: The drugs have a shelf life of four years, and they were proving ineffective for avian flu, which seemed to pose the greatest risk.

Some officials cited financial constraints, despite a 25 percent federal funding match for the antiviral medications.

"We purchased as much as we could with the funds we had," said Dena Iverson, spokeswoman for the District's health department.

Federal agencies were asked last year to create their own stockpiles. But the response has been uneven.

The Defense Department has stockpiled 8 million treatment courses for military service members and their families. The Postal Service, however, has no stockpile for its 330,000 mail carriers.

Even the agency in charge of the pandemic program, Health and Human Services, is behind schedule with its stockpiling effort. Last year, Robinson said, his department asked for \$2 million for antiviral medications for its workers, but none have been purchased.

<http://www.washingtonpost.com/wp-dyn/content/article/2009/04/30/AR2009043004265.html>

[\(Return to Articles and Documents List\)](#)

Daily Guardian

OPINION

April 28 2009

A Vaccine Needed for Bad Statistics: Eric Auchard

Reuters,

By Eric Auchard

LONDON, April 28 (Reuters) - If you look no further than the latest headlines, you might think a worldwide flu pandemic was already underway with a very real threat to millions of lives.

While there are many unanswered questions early on in the outbreak of flu from Mexico, it is crucial to remember that the number of deaths and reported infections remain small -- even if its spread across the globe has proved worryingly rapid.

While the infected need access to medical care and anti-viral drugs, the rest of the world needs an inoculation against scary statistics and misinformation.

The Internet Age allows facts and rumour to spread almost instantaneously. But knowing of outbreaks across the globe must not be confused with risks of catching the disease.

Already in this outbreak, Lebanon's health minister has called for a halt to the national custom of greeting one another with kisses. Several countries including Russia and China have banned pork imports from Mexico and parts of the United States in the belief that meat could spread the flu.

So far, up to 149 are reported to have died of swine flu in Mexico. The World Health Organisation has upgraded the level of pandemic threat to four on a scale of six -- sustained human-to-human transmission. Stage five signals an "imminent" pandemic.

However, influenza is a big killer every year, with or without a pandemic.

WHO estimates flu kills upward of 250,000 to 500,000 people year after year. "Normal" flu epidemics infect 3 to 5 million a year. Statistics are complicated by inconsistent reporting. Flu often leads to other ailments that end up being listed as the ultimate cause of death.

Flu's typical victims are the elderly, the infirm or the young. The difference with swine flu outbreak in Mexico is that otherwise healthy adults aged 20-50 are vulnerable.

But so far the new swine flu death rates are lower than other recent pandemic scares, a report by Barclays Capital notes. The 2,200 swine flu infections reported have resulted in deaths in 7 percent of cases. Avian flu has killed 61 percent of the 421 people infected since 1997. The death rate from SARS was around 10 percent.

Outside Mexico, 50 infections have been reported in the United States, Canada, Israel, New Zealand, Spain and Scotland. But health experts are baffled that infections outside Mexico appear to be milder and have caused no deaths.

The world's most recent flu pandemic 41 years ago was the 1968 Hong Kong outbreak, which claimed one million lives.

Historically, pandemics occur about three times a century. But like predictions of the next big earthquake, medical experts profess they have no idea when to expect the next pandemic.

Inevitably, comparisons end up turning back to the Spanish Flu of 1918-1920, which killed more than 50 million people, or 2.5 percent of the world's population.

That scourge followed the massive troop movements of World War One at a time of poor communications and before the invention of penicillin and modern healthcare systems. Post-war censorship rules restricted access to news, which limited the ability of communities to make informed decisions to protect themselves against the spread of the flu.

The descent into a global pandemic is not inevitable. Air travel may spread the disease in its early stages, but modern communications and medicine can arm us to respond quickly as the disease evolves.

<http://www.guardian.co.uk/business/feedarticle/8478428>

[\(Return to Articles and Documents List\)](#)

Washington Times

May 1, 2009

Bin Laden is Dead, Again

Osama bin Laden is dead, according to Pakistan's President Asif Ali Zardari. This week he stunned the world with the exciting news that Pakistan's intelligence services have "obviously" concluded that bin Laden "does not exist any more, that he is dead."

Au contraire, says Pakistani Taliban leader Sirajuddin Haqqani. "Osama bin Laden is still alive and is directing the jihad against American and Western forces in Afghanistan," he told the Saudi daily Al-Watan. But Mr. Haqqani admits he hasn't seen bin Laden lately. "It has been a long time since I lost contact with al Qaeda's leader," he said, but he remains confident that bin Laden is "still alive and leading al-Qaeda combatants against foreign forces."

We last heard from bin Laden on March 19 in his latest tape release, "Fight on, Champions of Somalia," which received the usual heavy media attention. The hunt is still on by the U.S. intelligence community. CIA Director Leon E. Panetta says he asks "every day" where bin Laden is hiding, and presumably he keeps getting the same answer. "The Americans tell me they don't know," Mr. Zardari said, "and they are much more equipped than us to trace him." Armed drones are flocking to remote Chitral in northwestern Pakistan, high in the Hindu Kush mountains, which intelligence reports indicate is the most probable hiding place.

Another suspect location is the picturesque town of Kalam, in the northernmost reaches of the Shariah-friendly Swat Valley. Swat Taliban spokesman Muslim Khan recently rolled out the welcome mat to al Qaeda. "Osama can come here," Mr. Khan said. "Sure, like a brother they can stay anywhere they want. Yes, we will help them and protect them."

It is regrettable that bin Laden is still at large 7 1/2 years after the Sept. 11, 2001, attacks. So long as he lives, he is a symbol and inspiration to his co-religionists, the terrorists who got away with murdering thousands of Americans and bringing war to our shores. For many years, Pakistan's former President Pervez Musharraf kept the United States at arm's length, stubbornly denying that bin Laden was in Pakistan and forbidding U.S. covert operations to settle the case. When Mr. Zardari took power late last summer, President George W. Bush authorized increased use of armed drones to track down and kill terrorist leaders inside Pakistan, and those operations have been remarkably effective.

Eleven of the top 20 terrorist targets have been taken out, prompting Pakistan to release a new Top 20 list. If he is alive, bin Laden cannot feel comfortable. But has he expired or not? "The question is whether he is alive or dead," Mr. Zardari said, getting back to basics. "There is no trace of him. But there is no evidence, you cannot take that as a fact." His bottom line? "We are between facts and fiction." In other words, we are back where we started. The hunt continues.

<http://washingtontimes.com/news/2009/may/01/bin-laden-is-dead-again/>

[\(Return to Articles and Documents List\)](#)