USAF COUNTERPROLIFERATION CENTER
CPC OUTREACH JOURNAL
MAXWELL AFB, ALABAMA

Issue No. 1051, 29 March 2013

Articles & Other Documents:

Featured Article: Reports Warn of Lax Inspections, Bioterror Lab Risks

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.

Issue No.1051, 29 March 2013

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.

United States Air Force Counterproliferation Research & Education | Maxwell AFB, Montgomery AL
Phone: 334.953.7538 | Fax: 334.953.7530

USAF COUNTERPROLIFERATION CENTER
CPC OUTREACH JOURNAL
MAXWELL AFB, ALABAMA

Al-Monitor – Washington, D.C.

'Most Substantive' Iran Nuclear Talks to Date, but Narrow Area of Agreement

March 26, 2013
By Laura Rozen

(Reuters) Iranian nuclear experts deeply engaged on the substance of a revised international proposal, and said they are considering suspending 20% enrichment for six months and converting their 20% stockpile to oxide for medical use at technical talks with six world powers held in Istanbul last week, diplomatic sources told Al-Monitor Tuesday.

However, the Iranians raised numerous objections to other elements in a revised international proposal presented in Kazakhstan last month, a diplomatic source, speaking not for attribution, said Tuesday. Among them: suspending other operations at Fordo except for 20% enrichment, shipping out Tehran's stockpile of 20% enriched fuel; as well as enhanced IAEA inspections.

American officials "had the most substantive conversation they ever had" with the Iranians, another analyst briefed on the Istanbul talks, speaking not for attribution, said. The Iranians "went through their [international] proposal slide by slide, and [the Iranians] didn't focus on [their] counter proposal."

The Iranians in Istanbul were cool to incentives in the revised offer, including modest sanctions relief, but did not explain what they would want instead, according to the diplomat.

The updated proposal offered to ease sanctions on the gold trade and petrochemical sales, but not major oil and banking sanctions, Al-Monitor reported last month.

Diplomats from six world powers head back to Almaty, Kazakhstan next week for political director level talks with Iran, to be held April 5-6.

Two sources suggested the US may be looking at additional incentives to possibly bolster the international offer, but the details were unclear.

The parties have said little publicly following the March 18 technical meeting in Turkey, in part perhaps due to the Persian New Year's (Nowruz) holiday underway and Easter and Passover holidays in the West.

But an Iranian source close to the talks on Tuesday pointed Al-Monitor to a speech by the Supreme Leader Ayatollah Khamenei last week for guidance on Tehran's negotiating stance.

"If the Americans wanted to resolve the issue, this would be a very simple solution: they could recognize the Iranian nation's right to enrichment and in order to address those concerns, they could enforce the regulations of the International Atomic Energy Agency," Khamenei said in a March 21 speech in the city of Mashhad. "We were never opposed to the supervision and regulations of the International Atomic Energy Agency."

"Whenever we are close to a solution, the Americans cause a problem in order to prevent reaching a solution," Khamenei continued. "My assumption and interpretation is that their goal is to keep the issue unresolved so that they can have a pretext for exerting pressure on us."

http://backchannel.al-monitor.com/index.php/2013/03/4872/most-substantive-talks-with-iran-in-istanbul-but-narrow-area-of-agreement/

(Return to Articles and Documents List)

Global Post – Boston, MA

UN Excludes Major Powers from Syria Chemical Arms Inquiry

Agence France-Presse (AFP)

March 26, 2013

The United Nations on Tuesday named a Swedish scientist to lead an inquiry into the alleged use of chemical weapons in Syria, but has barred experts from the major powers from taking part, officials said Tuesday.

UN leader Ban Ki-Moon appointed Ake Sellstrom of Sweden, a veteran of 1990s arms investigations in Iraq, to head the inquiry. No definitive mandate for the inquiry has been announced, although the UN said the aim is not to find who staged the alleged attacks.

Ban has told the UN Security Council permanent members -- the so-called P5 of Britain, China, France, Russia and United States -- that they will not be allowed to take part, diplomats said.

The decision was taken because of divisions over the worsening two-year-old war between President Bashar al-Assad's forces and opposition rebels, diplomats said.

Russia, Assad's main international backer, has made clear its irritation at being excluded. Russia expressed its "willingness" to take part in the investigation, Russia's UN ambassador, Vitaly Churkin, told reporters.

"We were told that the secretariat preferred to have a team which would exclude P5 members," he added.

"We do not fully share this kind of attitude but the main thing is for it to be as objective a team as possible," Churkin said. "So we will see what kind of group that will be and what will be the results of their work."

Syria asked for an investigation last week into its allegation that the opposition used chemical weapons in Aleppo on March 19. Britain and France have demanded that the inquiry also look into opposition accusations that the government used chemical arms in Aleppo and near Damascus.

Russia has strongly backed the Syria demand that the investigation be limited.

The UN has only said that the "initial focus" of the inquiry will be the Syrian government allegations.

UN spokesman Martin Nesirky said "the terms of reference for the mission are being finalized," including the composition of the inquiry team. No timetable has been set for the work to start.

"It is not a criminal investigation, it is a technical mission," said Nesirky. The investigators will be "aimed at ascertaining whether chemical weapons were used and not by whom."

Sellstrom, the head of the inquiry, is currently senior researcher at the European Center for Advanced Studies of Societal Security and Vulnerability, specializing in major incidents with chemical, biological, radiological, nuclear and explosive substances.

A renowned expert on disarmament and international security, Sellstrom was chief inspector with the UN Special Commission (UNSCOM) and also top adviser to the UN Monitoring, Verification and Inspection Commission (UNMOVIC) for Iraq.

He has taught at US universities and was also director of the Swedish Defense and Security Research Institute.

http://www.globalpost.com/dispatch/news/afp/130326/un-excludes-major-powers-syria-chemical-arms-inquiry

(Return to Articles and Documents List)

Times of Israel – Israel

'Iran may Freeze some Nuclear Activity to Ease Sanctions'

Islamic Republic said to be mulling parts of a Western proposal that would see 20% enrichment suspended for up to six months

By Stuart Winer
March 27, 2013

Iran may temporarily suspend some of its uranium enrichment activities in exchange for an easing of some of the Western-imposed sanctions aimed at curbing its nuclear program, diplomatic officials said on Tuesday.

Following the latest round of talks between Iranian and Western nuclear officials, which was held earlier this month in Istanbul, Turkey, Iranian officials said they would consider suspending 20-percent uranium enrichment activities for up to six months and converting existing stores of 20%-enriched nuclear material into oxide for medical use, the al-Monitor website reported on Tuesday.

However, the Iranians were said to be less flexible on other enrichment activities currently going on at the heavily fortified Fordo nuclear plant. Iran also ruled out increased International Atomic Energy Commission inspection of its nuclear facilities, the report said.

An analyst told the website that American officials who participated in the Istanbul talks "had the most substantive conversation they ever had" with the Iranian representatives.

The revised proposals came after an earlier round of talks in Kazakhstan ended without any real progress.

If Iran accedes to the demands of the P5+1 — the six world powers that are attending the talks: the US, China, Russia, France, Britain and Germany — sanctions on Iran's petrochemical and gold sectors would be eased, while restrictions on banking and petrolium sales would remain in place, the report said.

Diplomats from the P5+1 and Iran were scheduled to reconvene in Kazakhstan on April 5-6 for continued talks, which the United States and its allies hope will bring to an end Iran's nuclear program. Last week, during his visit to Israel, US President Barack Obama vowed that he would do "whatever is necessary" to prevent Iran from developing nuclear weapons.

http://www.timesofisrael.com/iran-may-freeze-some-nuclear-activity-to-ease-sanctions/

(Return to Articles and Documents List)

The London Daily Telegraph – U.K.

North Korea 'Defeats' US Troops in New Video

The latest propaganda video to emerge from North Korea depicts paratroopers descending on Seoul in an invasion scenario that it said would see thousands of US citizens living in South Korea taken hostage.

Agence France-Presse (AFP)
24 March 2013

The four-minute video, titled "A Short, Three-Day War," begins with images of a massive artillery and rocket barrage, followed by a large-scale land and air assault with North Korean troops streaming over the border.

The video was posted on the North's official website, Uriminzokkiri, which distributes news and propaganda from the state media.

The video's male narrator describes different stages of the invasion, including the destruction of forces under the US Pacific Command with "powerful weapons of mass destruction."

"The crack stormtroops will occupy Seoul and other cities and take 150,000 US citizens as hostages," he says.

The video shows footage of paratroopers jumping from the sky superimposed over an aerial shot of the South Korean capital, with North Korean military helicopters hovering overhead.

South Korea has a large US expatriate population, as well as 28,000 US troops based in the country.

The video was the latest in a line of similarly-themed productions posted to the Uriminzokkiri channel.

An video released early last month showed New York in flames after an apparent missile attack, and another two weeks later depicted US soldiers and President Barack Obama burning in the flames of a nuclear blast.

And earlier this week, another video showed the dome of the US Capitol building in Washington exploding in a fireball.

The latest offering from the Pyongyang propaganda department comes during escalating tensions on the Korean peninsula, with multiple threats from Pyongyang of an armed response to joint South Korea-US military drills and to UN sanctions imposed after its nuclear test last month.

On Thursday, the North Korean military threatened strikes on US military bases in Japan and Guam.

It has since followed this threat up by announcing that its military has been put on "highest alert" for possible strikes against the US.

http://www.telegraph.co.uk/news/worldnews/asia/northkorea/9947489/North-Korea-defeats-US-troops-in-new-video.html

(Return to Articles and Documents List)

Washington Examiner

Experts: NKorea Training Teams of 'Cyber Warriors'

By Associated Press (AP)
March 24, 2013

SEOUL, South Korea (AP) — Investigators have yet to pinpoint the culprit behind a synchronized cyberattack in South Korea last week. But in Seoul, the focus is fixed on North Korea, which South Korean security experts say has been training a team of computer-savvy "cyber warriors" as cyberspace becomes a fertile battleground in the nations' rivalry.

Malware shut down 32,000 computers and servers at three major South Korean TV networks and three banks last Wednesday, disrupting communications and banking businesses. The investigation into who planted the malware could take weeks or even months.

South Korean investigators have produced no proof yet that North Korea was behind the cyberattack. Some of the malware was traced to a Seoul computer. Without elaborating, police said Monday that some of the malicious code also came from the United States and three European countries, South Korea's Yonhap news agency reported. But South Korea has pointed the finger at Pyongyang in six cyberattacks since 2009, even creating a cybersecurity command center in Seoul to protect the Internet-dependent country from hackers from the North.

It may seem unlikely that impoverished North Korea, with one of the most restrictive Internet policies in the world, would have the ability to threaten affluent South Korea, a country considered a global leader in telecommunications. The average yearly income in North Korea was just $1,190 per person in 2011 — just a fraction of the average yearly income of $22,200 for South Koreans that same year, according to the Bank of Korea in Seoul.

But for several years, North Korea has poured money into science and technology. In December, scientists succeeded in launching a satellite into space aboard a long-range rocket from its own soil. And in February, North Korea conducted its third nuclear test.

"IT" has become a buzzword in North Korea, which has developed its own operating system called Red Star. The regime also encouraged a passion for gadgets among its elite, introducing a Chinese-made tablet computer for the North Korean market. Teams of developers came up with software for everything from composing music to learning how to cook.

But South Korea and the U.S. believe North Korea also has thousands of hackers trained by the state to carry its warfare into cyberspace, and that their cyber offensive skills are as good as or better than their counterparts in China and South Korea.

"The newest addition to the North Korean asymmetric arsenal is a growing cyber warfare capability," James Thurman, commander of the U.S. forces in South Korea, told U.S. legislators in March 2012. "North Korea employs sophisticated computer hackers trained to launch cyber-infiltration and cyber-attacks" against South Korea and the U.S.

In 2010, Won Sei-hoon, then chief of South Korea's National Intelligence Service, put the number of professional hackers in North Korea's cyber warfare unit at 1,000.

North Korean students are recruited to the nation's top science schools to become "cyber warriors," said Kim Heung-kwang, who said he trained future hackers at a university in the industrial North Korean city of Hamhung for two decades before defecting in 2003. He said future hackers also are sent to study abroad in China and Russia.

In 2009, then-leader Kim Jong Il ordered Pyongyang's "cyber command" expanded to 3,000 hackers, he said, citing a North Korean government document that he said he obtained that year. The veracity of the document could not be independently confirmed.

Kim Heung-kwang, who has lived in Seoul since 2004, speculated that more have been recruited since then, and said some are based in China to infiltrate networks abroad.

What is clear is that "North Korea has a capacity to send malware to personal computers, servers or networks and to launch DDOS-type attacks," he said. "Their targets are the United States and South Korea."

Expanding its warfare into cyberspace by developing malicious computer codes is cheaper and faster for North Korea than building nuclear devices or other weapons of mass destructions. The online world allows for anonymity because it is easy to fabricate IP addresses and destroy the evidence leading back to the hackers, according to C. Matthew Curtin, founder of Interhack Corp.

Thurman said cyberattacks are "ideal" for North Korea because they can take place relatively anonymously. He said cyberattacks have been waged against military, governmental, educational and commercial institutions.

North Korean officials have not acknowledged allegations that computer experts are trained as hackers and have denied many of the cyberattack accusations. Pyongyang has not commented on the most recent widespread attack in South Korea.

In June 2012, a seven-month investigation into a hacking incident that disabled news production system at the South Korean newspaper JoongAng Ilbo led to North Korea's government telecommunications center, South Korean officials said.

In South Korea, the economy, commerce and every aspect of daily life is deeply dependent on the Internet, making it ripe grounds for a disruptive cyberattack.

North Korea, in contrast, is just now getting online. Businesses are starting to use online banking services, and debit cards have grown in popularity. But only a sliver of the population has access to the global Internet, meaning an Internet outage two weeks ago — which Pyongyang blamed on hackers from Seoul and Washington — had little bearing on most North Koreans.

"North Korea has nothing to lose in a cyber battle," said Kim Seeongjoo, a professor at Seoul-based Korea University's Department of Cyber Defense. "Even if North Korea turns out to be the attacker behind the broadcasters' hacking, there is no target for South Korean retaliation."

Associated Press writer Jean H. Lee contributed to this story with reporting from Pyongyang, North Korea; Hyung-jin Kim in Seoul also contributed to this report.

http://washingtonexaminer.com/experts-nkorea-training-teams-of-cyber-warriors/article/feed/2082311

(Return to Articles and Documents List)

Times of India – India

USAF COUNTERPROLIFERATION CENTER
CPC OUTREACH JOURNAL
MAXWELL AFB, ALABAMA

Top China College Linked to PLA's Cyberspying Unit

By Reuters
March 25, 2013

SHANGHAI: Faculty members at a top Chinese university have collaborated for years on technical research papers with a People's Liberation Army (PLA) unit accused of being at the heart of China's alleged cyberwar against Western commercial targets.

Several papers on computer network security and intrusion detection, easily accessed on the internet, were co-authored by researchers at PLA Unit 61398, allegedly an operational unit actively engaged in cyberespionage, and faculty at Shanghai Jiaotong University, a centre of academic excellence with ties to some of the world's top universities and attended by the country's political and business elite.

The apparent working relationship between the PLA unit and Shanghai Jiaotong is in contrast to common practice in most developed nations, where university professors in recent decades have been reluctant to cooperate with operational intelligence gathering units.

The issue of cybersecurity is testing ties between the world's two biggest economies, prompting US President Barack Obama to raise concerns over computer hacking in a phone call with new Chinese President Xi Jinping. China denies it engages in state-sponsored hacking, saying it is a victim of cyberattacks from the United States.

There is no evidence to suggest any Shanghai Jiaotong academics who co-authored papers with Unit 61398 worked with anyone directly engaged in cyberespionage operations, as opposed to research.

"The issue is operational activity - whether these research institutions have been involved in actual intelligence operations," said James Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies. "That's something the US does not do."

"(In the US) there's a clear line between an academic researcher and people engaged in operational (intelligence gathering) activities."

Shanghai Jiaotong declined to comment.

Co-authors

In reviewing the links between the PLA and Shanghai Jiaotong - whose alumni include former President Jiang Zemin, the head of China's top automaker and the former CEO of its most popular internal portal - Reuters found at least three papers on cyberwarfare on a document-sharing website that were co-authored by university faculty members and PLA researchers.

The papers, on network security and attack detection, state on their title pages they were written by Unit 61398 researchers and professors at Shanghai Jiaotong's School of Information Security Engineering (SISE).

In one 2007 paper on how to improve security by designing a collaborative network monitoring system, PLA researcher Chen Yi-qun worked with Xue Zhi, the vice-president of SISE and the school's Communist Party branch secretary. According to his biography on the school's website, Xue is credited with developing China's leading infiltrative cyberattack platform.

Calls and emails to Xue were not answered. Reuters was unable to find contact details for Chen.

Fan Lei, an associate professor at Shanghai Jiaotong whose main research areas are network security management and cryptography, also co-authored a paper with Chen. Fan told Reuters he has no links with Unit 61398 and his work with Chen in 2010 was because Chen was a SISE graduate student. Fan said he was unaware Chen was with the PLA when they collaborated. Both of the papers Chen co-wrote with SISE professors stated he was with the PLA unit.

Cybersecurity experts say the publicly available papers and China's National Information Security Engineering Centre are ostensibly about securing computer networks.

"The research seems to be defensive, but cybersecurity research in general can be dual purpose," said Adam Meyers, director of intelligence at CrowdStrike, a security technology company based in Irvine, California. Figuring out how best to defend networks, by definition, means thinking about the most effective means of attack, he noted.

Efforts to reach the PLA for comment on its collaboration with Shanghai Jiaotong were unsuccessful.

Tech park neighbours

Set amid manicured lawns, Shanghai Jiaotong University is one of China's top four colleges, turning out brilliant technical engineers much in demand by both domestic companies and foreign multinationals. Its reputation has led to tie-ups with elite universities abroad.

Last month, Mandiant, a private US-based security firm, accused China's military of cyber-espionage on US and other English-speaking companies, identifying Unit 61398 and its location at a building on the outskirts of Shanghai. China said the report was baseless and lacked "technical proof".

"SISE at Shanghai Jiaotong has provided support" to PLA Unit 61398 - known more formally as General Staff Department (GSD), Third Department, Second Bureau - said Russell Hsiao, author of papers on China's cyberwarfare capabilities for Project 2049 Institute, a Virginia-based think-tank, who drew his research from the technical papers and government reports.

He said another Shanghai Jiaotong department, the Department of Computer Science and Engineering, also did research work with another PLA unit. A Project 2049 report last year found the GSD's Third Department had oversight of "information security engineering bases" in Shanghai, Beijing and Tianjin.

The GSD Third Department's Shanghai base is in an industrial park housing mainly government research institutes and high-tech firms. The SISE building is in the same development, 40 kms from the university's main Minhang campus. Across the street from SISE is the National Information Security Engineering Center, a building commissioned in 2003 by PLA Unit 61398. Also part of the base is the Ministry of Public Security's Third Research Institute, which researches digital forensics and network security.

Auto research

Shanghai Jiaotong is not officially linked to China's military. SISE says on its website its goal is to speed up the development of China's information security sector and address the national shortage of information security professionals.

Shanghai Jiaotong set up a joint institute in China's second city in 2006 with the University of Michigan - seeking, it says on its web site, to "develop innovative and highly reputable education and research programs in various engineering fields." A spokesman for the US college said it has no relationship with SISE. Carnegie Mellon University in Pittsburgh also had a partnership with Shanghai Jiaotong's School of Electronic, Information and Electrical Engineering, and Singapore Management University said it ended a tie-up with SISE last June.

Among the industries in the United States allegedly targeted by Unit 61398, as recently as last year according to Mandiant, is transportation, including the auto sector.

The University of Michigan collaborates closely with Detroit-based automakers on research projects, and is one of three colleges that comprise the University Research Corridor, which spent $300 million on R&D projects over the last five years. Nearly a third of that was funded by private industry, according to local consultant the Anderson Economic Group.

"There was no indication in 2010 that the joint institute was involved in any way and that also is the case today. We do, of course, watch the news reports on these issues carefully," said Rick Fitzgerald, a University of Michigan spokesman,

referring to a New York Times report in 2010 citing investigators' claims to have tracked cyberattacks against Google to Shanghai Jiaotong and an eastern Chinese vocational school.

http://articles.timesofindia.indiatimes.com/2013-03-25/internet/38009364_1_network-security-top-china-papers

(Return to Articles and Documents List)

Asahi Shimbun – Japan

U.S., South Korea Strengthen Response to North Korea's Provocations

March 25, 2013
By AKIHIKO KAISE/ Correspondent

SEOUL—The United States has signed an agreement to join South Korean military operations conducted in response to provocations by North Korea, officials in Seoul said March 24.

The South Korean and U.S. militaries had already signed a similar joint operational plan to prepare for an all-out war on the Korean Peninsula, but it assumes South Korea would deal with local provocations alone.

The latest joint operational plan widens that cooperation and is intended to deter North Korea's belligerence. If Pyongyang takes any provocative action near the military boundary or in other regions, U.S. forces would support countermeasure operations led by the South Korean military.

"By completing this plan, we improved our combined readiness posture to allow us to immediately and decisively respond to any North Korean provocation," a South Korean official said.

Seoul and Washington started preparing to draw up a new joint operational plan after North Korea shelled the South Korean island of Daeyeonpyeongdo near the military boundary in November 2010. Four people were killed, including two civilians, and about 20 were injured in the attack.

The latest operational plan was signed on March 22 by Jung Seung-jo, chairman of South Korea's joint chiefs of staff, and James Thurman, commander of the U.S. forces in South Korea.

Thurman said the completion of the plan underlines the strength of the U.S.-South Korea alliance.

A military source said the latest plan could make Pyongyang think twice about its actions.

"North Korea cannot easily attack the U.S. military," the source said. "If the U.S. military intends to respond to local provocations in earnest, the deterrence effect would become much greater."

http://ajw.asahi.com/article/asia/korean_peninsula/AJ201303250105

(Return to Articles and Documents List)

The Hankyoreh – South Korea

President Park Asks N. Korea to Give Up its Nukes

On third anniversary of Cheonan sinking, Park calls for a calming of the tensions currently on the peninsula
March 27, 2013
By Cho hye-jeong, staff reporter

On Mar. 26, South Korean President Park Geun-hye said, "The only way for North Korea to survive is to voluntarily lay down its nuclear weapons, its missiles, its threats and provocations and become a responsible member of the international community."

Park spoke at a morning memorial service held at the Daejeon National Cemetery on the third anniversary of the sinking of the Cheonan warship. "We earnestly ask North Korea to change," she said. "They must hurry to disabuse themselves of the notion that nuclear weapons will preserve their regime."

"North Korea must immediately cease these provocations, which burden the young generation of Koreans with a vicious cycle of sacrifice and confrontation. It must instead choose to open a virtuous cycle of peace and prosperity for the Korean peninsula."

Park also repeatedly issued warnings. "Concentrating the country's resources on developing nuclear weapons to preserve the regime while its people are struggling to keep food on the table will only lead to North Korea's international isolation."

"The strongest thing that can protect a country is the people's clear awareness of security and unity. As I see it, when the security of the nation is at stake, the differences separating us disappear, and the gap between liberals and conservatives is bridged," she added."

Before the memorial service, Park first talked with about 60 of the sailors' bereaved family members and then placed flowers on the graves. As the names of the 46 sailors who died during the sinking of the Cheonan were read one by one in a video that played during the memorial service, Park's eyes welled with tears.

In a command letter issued to his subordinate units on the same day, Minister of Defense Kim Kwan-jin said," Only our firm posture of readiness and our clear preparedness to retaliate can deter enemy provocations. Let us remember the spirit of sacrifice of the brave sailors on the Cheonan and adopt an even firmer posture to defend the nation."

"When I think of the heroes on the Cheonan who died beneath the cold ocean waves, even now I think my heart is going to break," he added. "The sinking of the Cheonan reminded us that nothing has changed about North Korea's bellicosity and its ambition to spread communism to South Korea."

http://english.hani.co.kr/arti/english_edition/e_northkorea/579978.html

(Return to Articles and Documents List)

Yonhap News Agency – South Korea
March 27, 2013

N. Korea Warns Pre-Emptive Nuclear Attack part of its Military Options

SEOUL, March 27 (Yonhap) -- North Korea on Wednesday said launching a pre-emptive nuclear attack on the U.S. and South Korea is part of its military options as the country ratcheted up its warlike rhetoric amid escalating tensions over the North's recent nuclear test and joint military drills carried out by the two allies.

North Korea's military said Tuesday that it will put its missile and artillery units into the highest-level combat readiness posture, fueling further the already-tense inter-Korean relations. The country also reiterated its threat to take actual military actions.

http://english.yonhapnews.co.kr/news/2013/03/27/0200000000AEN20130327005500315.HTML

(Return to Articles and Documents List)

South China Morning Post – Hong Kong, China

'Combat-Ready' North Korea Threatens Hawaii, US Mainland

Guam also under threat as units 'placed under class-A combat readiness'
Wednesday, 27 March, 2013
By Agence France-Presse (AFP)

North Korea's military put its "strategic" rocket units on a war footing Tuesday, with a fresh threat to strike targets on the US mainland, Hawaii and Guam, as well as South Korea.

"All artillery troops including strategic rocket units and long-range artillery units are to be placed under class-A combat readiness," the Korean People's Army supreme command said in a statement.

The units should be prepared to attack "all US military bases in the Asia-Pacific region, including the US mainland, Hawaii and Guam" and South Korea, said the statement carried by the Korean Central News Agency.

Despite a successful long-range rocket launch in December, most experts believe North Korea is years from developing a genuine inter-continental ballistic missile that could strike the mainland United States.

Hawaii and Guam would also be outside the range of its medium-range missiles, which would be capable, however, of striking US military bases in South Korea and Japan.

The supreme command announcement came days after the South Korean and US militaries signed a new pact, providing for a joint military response to even low-level provocative action by North Korea.

While existing agreements provide for US engagement in the event of a full-scale conflict, the new protocol addresses the response to a limited provocation such as an isolated incident of cross-border shelling.

It guarantees US support for any South Korean retaliation and allows Seoul to request any additional US military force it deems necessary.

Military tensions on the Korean peninsula have been at an elevated level for months, following December's rocket test and the North's third nuclear test which it carried out last month.

Both events triggered UN sanctions that infuriated the North, which has spent the past month issuing increasingly threatening statements about unleashing an "all-out war" backed by nuclear weapons.

Some have included similar warnings of looming strikes on US bases in the Pacific region, including Guam.

North Korea was particularly incensed that nuclear-capable US B-52 bombers flying out of Andersen Air base on Guam took part in recent joint South Korea-US military exercises.

"We will demonstrate the firm resolution of our people and military to protect our sovereignty and dignity through real military action," Tuesday's statement warned.

"There is no greater delusion than the idea that they will have an opportunity for retaliation," it added.

The statement coincided with the third anniversary of the sinking of a South Korean naval vessel by what Seoul insists was a North Korean submarine. Pyongyang has always denied any involvement.

Addressing a memorial ceremony for the 46 sailors who died in the incident, South Korean President Park Geun-Hye warned North Korea that its only "path to survival" lay in abandoning its nuclear and missile programmes.

Sabre-rattling and displays of brinkmanship are nothing new in the region, but there are concerns that the current situation is so volatile that one accidental step could escalate into serious conflict.

http://www.scmp.com/news/asia/article/1200215/now-combat-ready-north-korea-threatens-hawaii-and-us-mainland-long-range

(Return to Articles and Documents List)

The Korea Herald – South Korea

N. Korea Cuts Inter-Korean Military Hotline

March 27, 2013

North Korea said Wednesday that it will cut a military hotline with South Korea, the latest in a string of provocations that include the North's unilateral severance of an inter-Korean Red Cross hotline about two weeks ago.

"The Supreme Command of the Korean People's Army solemnly declared that... Due to the reckless acts of the enemies, the north-south military communications which were set up for dialogue and cooperation between the north

and the south has already lost its significance," the North's Korean Central News Agency said in a report, citing hostility from the United States and South Korea.

The report said that the North sent a message to the South at 11:20 a.m., quoting the head of the North Korean side's delegation to the north-south general-level military talks as saying, "I, upon authorization, inform the south side that the north-south military communications will be cut off and the members of the north side at the military communications liaison office in the zone under the control of the north and the south in the west coastal area will stop their activities from this moment."

Earlier on March 11, the communist North disconnected the inter-Korean Red Cross hotline that ran through the truce village of Panmunjom.

The latest move is feared to affect the operation of the inter-Korean industrial complex in the North's border town of Kaesong, as the west coastal military hotline is responsible for guaranteeing the safety of South Korean personnel commuting to and from the Kaesong complex, according to analysts in Seoul.

The military hotline has been used to notify the North of any planned movement of people and vehicles to the Kaesong complex located just north of the demilitarized zone that separates the two Koreas.

Pyongyang also said earlier in the month that it will nullify the Armistice Agreement that halted the Korean War and no longer respect non-aggression pacts reached between the two Koreas in the past. (Yonhap News)

http://www.koreaherald.com/view.php?ud=20130327000971

(Return to Articles and Documents List)

RIA Novosti – Russian Information Agency

Nuclear-Capable US Bombers Fly Over S. Korea

28 March 2013

WASHINGTON, March 28 (RIA Novosti) The US military said Thursday it had sent two nuclear-capable B-2 stealth bombers on an “extended deterrence” practice run over South Korea, dropping dummy bombs as part of a bilateral training exercise.

“This mission… demonstrates the United States’ ability to conduct long range, precision strikes quickly and at will,” said a statement from the United States Forces Korea, a division of the US Strategic Command under the Department of Defense.

While it is unclear if US stealth bombers had been used in previous military drills with South Korea, this was the first time the military announced their use, the Associated Press reported.

The two bombers, capable of carrying both conventional and nuclear weapons, left the Whiteman Air Force Base in Missouri and flew more than 6,500 miles (10,461 km) to the Korean Peninsula where they dropped the inert munitions on an island range facility off the western coast of South Korea, and then returned to the United States “in a single, continuous mission,” according to the statement.

The flight was "intended to demonstrate very clearly the resolve of the United States to deter against aggression on the Korean Peninsula, and our strong commitment to the US alliance with South Korea," a senior defense official told CBS News.

The point was underscored in a phone call Wednesday night between US Secretary of Defense Chuck Hagel and South Korean Defense Minister Kim Kwan-jin.

"Secretary Hagel and Minister Kim reaffirmed the strength of the alliance, which has been, and continues to be, instrumental in maintaining stability on the Korean Peninsula,” Pentagon Press Secretary George Little said in a statement.

The bombing mission comes in the midst of escalating tensions between the United States and North Korea.

Earlier this month a spokesman for the North Korean Foreign Ministry threatened a pre-emptive nuclear strike against the United States after the United Nations Security Council approved sanctions in response to a third nuclear test by North Korea in February.

The US military announced earlier this month that it would strengthen its missile defenses in response to threats from North Korea.

“The United States is steadfast in its alliance commitment to the defense of the Republic of Korea, to deterring aggression, and to ensuring peace and stability in the region,” said the statement from the United States Forces Korea released Thursday.

The bombing run was part of a training exercise between US and South Korean forces that started March 1 and continues through the end of April.

http://en.rian.ru/military_news/20130328/180304311.html

(Return to Articles and Documents List)

Yonhap News Agency – South Korea
March 29, 2013

N.K. Leader Orders Rocket Forces to be on Standby to Strike U.S. and S. Korean Targets

SEOUL, March 29 (Yonhap) -- North Korean leader Kim Jong-un ordered the country's strategic rocket forces to be placed on standby to strike U.S. and South Korean targets, state media reported Friday, after two B-2 stealth bombers conducted first-ever operational drills over the Korean Peninsula.

The Korean Central News Agency (KCNA) said, in an English dispatch, "(Kim) convened an urgent operation meeting on the Korean People's Army's Strategic Rocket Force's performance of duty for firepower strike at the Supreme Command at 00:30 Friday.

"He finally signed the plan on technical preparations of strategic rockets, ordering them to be on standby to fire so that they may strike any time the U.S. mainland, its military bases in the operational theaters in the Pacific, including Hawaii and Guam, and those in south Korea," the report said.

It added that Kim pointed out that by letting B-2s make sorties over the South, the U.S. once again showed its hostile intent against the North and claimed Washington's provocation has entered a reckless level, "going beyond the phase of threat and blackmail."

The KCNA said that Kim viewed the B-2 bombing drills as more than simple demonstration of force in reaction to the tough stance by North Korea, but an ultimatum that Washington will ignite a nuclear war at any cost.

"Kim declared the revolutionary armed forces of the DPRK would react to the U.S. nuclear blackmail with merciless nuclear attack, and war of aggression with an all-out war of justice (of its own)," the KCNA said. The DPRK stands for the Democratic People's Republic of Korea, the North's official name.

Meanwhile, the swift reporting of a middle of the night emergency meeting of senior commanders is unusual and may reflect the level of intimidation felt by Pyongyang with the appearance of the B-2s over South Korea.

The U.S. Air Force's nuclear-capable stealth bombers carried out their bombing drill over the Korean Peninsula, hitting Jik Islet off Gunsan with bombs on Thursday. The move is seen as a clear message of strong warning to Pyongyang, which has recently threatened a pre-emptive nuclear attack on the U.S. and South Korea.

The North ratcheted up tension by launching a long-range rocket late last year and by detonating its third nuclear device on Feb. 12, in the face of strong opposition from the international community.

The planes took off from Whiteman Air Force Base in Missouri on Wednesday and flew over 10,000 kilometers using airborne refueling to reach South Korea the following day. The bombers can each carry up to 23 tons or various guided bombs and are designed to penetrate heavily defended air space to strike key targets such as command and control facilities without being detected by radar.

South Korea views the North's bluster as a response to the bombing exercise, an official said.

"A B-2 stealth strategic bomber conducted a bombing exercise over the Korean Peninsula yesterday," the presidential official said. "Though this bombing exercise is part of routine drills between South Korea and the U.S., we take First Chairman Kim's order as a step to respond to this (exercise)."

The official also said the government is carefully handling the situation.

http://english.yonhapnews.co.kr/northkorea/2013/03/29/69/0401000000AEN20130329001351315F.HTML

(Return to Articles and Documents List)

Economic Times – India

China Defends Deal to Build 1000 MW Nuclear Plant for Pakistan

By Press Trust of India (PTI)
March 25, 2013

BEIJING: Tacitly confirming reports of signing of an agreement with Pakistan to build a huge 1000 MW nuclear power plant, China today defended the deal saying that it confirmed to safeguards of the IAEA and rejected allegations that it has violated NSG norms.

"China has noted the relevant report", Chinese Foreign Ministry spokesman Hong Lei told a media briefing here today.

He was replying to a question on reports from Washington that Beijing has secretly entered a deal with Pakistan to construct the plant at Chashma in Punjab province.

On allegations that the deal violated the norms set by 46 member Nuclear Suppliers Group (NSG), which regulates the issues relating to nuclear proliferation and commerce, Hong said, "I want to point out that relevant cooperation between China and Pakistan does not violate relevant norms of the NSG".

In recent years China and Pakistan have had some cooperation in the field of civilian nuclear cooperation, he said.

All this cooperation is for peaceful use and this cooperation is in compliance with our respective international obligations and subject to the safeguards of the IAEA, Hong said.

A Washington-based news report had said two days ago that China has secretly signed the deal to construct a new power plant at Chashma.

China has so far aided and assisted Pakistan in constructing four power plants at Chashma.

Chashma I and II were stated to be 300 MW each and as per the previous plans the III and IV were stated to have 340 MW each.

While I and II were already commissioned, three and four were expected to be commissioned in 2016.

It is not clear whether the 1000 MW reactor would be a fifth one to be constructed there or the third reactor would be upgraded.

China argues that the new 1000 MW plant which it refers one Giga-watt reactor was "grandfathered" by a previous agreement that led to the construction and operation of earlier nuclear power plants at Chashma.

According to the US media report, the China-Pakistan agreement calls for the state-run China National Nuclear Corporation (CNNC) to construct a 1,000-megawatt power plant at Chashma.

The Washington Free Beacon quoted unnamed state department official as saying the Chinese move would be in violation of its promise to the NSG. China, which joined NSG in 2005, agreed not to sell additional reactors to Pakistan beyond the two reactors sold earlier.

"NSG participating governments have discussed the issue of China's expansion of nuclear cooperation with Pakistan at the last several NSG plenary sessions," a state department official was quoted as saying.

"We remain concerned that a transfer of new reactors at Chashma appears to extend beyond the cooperation that was 'grandfathered' in when China was approved for membership in the NSG," the official told the Beacon, which reported that the US is expected to protest the sale at an upcoming NSG meeting in June.

India too in the past has expressed its concerns to Beijing over China's nuclear engagement with Pakistan.

China's move to build a new plant comes after it developed an indigenous one Gigawatt plant of its own.

Though China has constructed several of 1000 MW nuclear plants, most of them were based on the foreign technology, specially, that of Japan, France and US.

China could not export the 1000 MW reactor technology to Pakistan due to objections from foreign suppliers.

Last November, China said it has rolled out its advanced 1,000 MW pressurised water nuclear power reactor, ACPR-1000 at the Hi-Tech Fair in Shenzhen.

The reactor was "independently" developed by China Guangdong Nuclear Power Corporation with full IPR and made its debuted at the 13th China Hi-Tech Fair, according to the official media.

http://articles.economictimes.indiatimes.com/2013-03-25/news/38010065_1_china-national-nuclear-corporation-chashma-china-and-pakistan

(Return to Articles and Documents List)

Times of India – India

India Readies Hi-Tech Naval Base to Keep Eye on China

By Rajat Pandit, Tamil News Network (TNN)
March 26, 2013

NEW DELHI: Slowly but steadily, India's new futuristic naval base is beginning to take concrete shape on the eastern seaboard. The strategic base, with an eye firmly on China, will eventually even have underground pens or bunkers to protect nuclear submarines both from spy satellites and enemy air attacks.

Sources said a flurry of discussions and meetings have been held in the PMO and defence ministry over the last couple of months to firm up "expansion plans'' for a base located near Rambilli called "Project Varsha" on the Andhra coast just about 50 km from the Eastern Naval Command headquarters at Visakhapatnam over the coming decade.

Though it's still very early days for Project Varsha, some bill it as an answer to China's massive underground nuclear submarine base at Yalong on the southernmost tip of Hainan Island, which houses its new Shang-class SSNs (nuclear-powered attack submarines) and the Jin-class SSBNs (nuclear-powered submarines with long-range nuclear missiles).

Although land acquisitions and incremental development work on the base under the secretive project kicked off a few years ago, it is set to take off in a major way with the construction of tunnels, jetties, depots, workshops and accommodation. "Further land acquisitions for the sprawling base to be spread over 20 sq km are now underway, with long-term budget allocations also being planned,'' said a source.

The endeavour dovetails into the overall policy to bolster force-levels on the eastern seaboard, with new warships, aircraft and spy drones as well as forward-operating (FOBs) and operational turnaround (OTR) bases, to counter China's expanding footprint in the entire Indian Ocean Region (IOR).

Naval assets to protect India's long coastline and keep watch over the crucial trade corridors in the Indian Ocean are essential to Indian interests. The strategic value of force projection beyond the Andaman islands is seen in terms of deterrence as well given the aggressive military Chinese expansion. India's own SSBN programme is also poised to turn the corner soon with sea trials of the 6,000-tonne INS Arihant slated to begin off Visakhapatnam. INS Arihant and its three "follow-on'' SSBNs, which will complete India's elusive nuclear weapon triad since they will be armed with the `K' series of submarine-launched ballistic missiles, as well as other frontline warships will be housed at the new base.

The Navy plans to operate at least three SSBNs and six SSNs in the long run for effective nuclear deterrence. Moreover, after inducting the 8,140-tonne INS Chakra submarine on a 10-year lease from Russia last year, India is now negotiating the lease of another such nuclear-powered Akula-II class submarine, as was earlier reported by TOI.

Project Varsha's ambitious scale in the years ahead will rival the expansive "Project Seabird'' under which the Karwar naval base has come up in coastal Karnataka to give India both strategic depth and operational flexibility on the western seaboard against Pakistan. While Karwar will decongest the over-crowded Mumbai port, the new base will do the same for Vizag on the east.

Karwar can currently base 11 major warships and 10 yard-craft after completion of its Phase-I at a cost of Rs 2,629 crore. The Cabinet Committee on Security (CCS) had last year approved Rs 13,000 crore for its expansion under Phase-IIA to ensure it can berth 32 major warships and submarines by 2018-19.

Karwar will be the home base for aircraft carrier INS Vikramaditya, the 44,570-tonne Admiral Gorshkov being refitted in Russia for $2.33 billion, as well as the six French Scorpene submarines being built at Mazagon Docks for Rs 23,562 crore.

http://articles.timesofindia.indiatimes.com/2013-03-26/india/38039841_1_akula-ii-ins-chakra-underground-nuclear-submarine-base

(Return to Articles and Documents List)

RIA Novosti – Russian Information Agency

US, Russian Defense Chiefs Agree to Resume Missile Defense Talks

26 March 2013

WASHINGTON, March 26 (RIA Novosti) - Russian and US defense chiefs during a phone conversation on Monday agreed to resume missile defense talks at the deputy minister level, the office of the Pentagon Press Secretary George Little said in a statement.

According to the readout of the conversation between Russian Defense Minister Sergey Shoigu and US Secretary of Defense Chuck Hagel, posted on the department’s official website, the Russian minister “expressed his desire to reconvene missile defense discussions with the U.S. at the deputy minister level” during the phone

“Secretary Hagel agreed and reiterated that this is an important part of U.S.-Russian relations. He assured Minister Shoigu that these discussions would continue and be carried forward by Under Secretary of Defense for Policy Dr. Jim Miller,” the statement reads.

Russia and NATO initially agreed to cooperate on the so-called European missile defense system at the Lisbon summit in November 2010. Further talks between Moscow and the alliance have foundered over NATO’s refusal to grant Russia legal guarantees that the system would not be aimed against Russia’s strategic nuclear deterrent.

NATO and the United States insist the shield is designed to defend NATO members against missiles from emerging threat nations like North Korea and Iran, and would not be directed at Russia. The alliance has vowed to continue developing and deploying its missile defenses, regardless of the status of missile defense cooperation with Russia.

http://en.rian.ru/russia/20130326/180252911/US-Russian-Defense-Chiefs-Agree-to-Resume-Missile-Defense-Talks.html

(Return to Articles and Documents List)

RIA Novosti – Russian Information Agency

Russia to Equip Submarine Forces with High-Precision Weapons

27 March 2013

VILYUCHINSK, March 27 (RIA Novosti) – Russia plans to equip its submarine forces with long-range high-precision weapons, which will enhance their strategic deterrent capabilities, Russia's defense minister said Wednesday.

"There are plans to equip the submarine forces with long-range high-precision weapons. This will significantly enhance the possibility of using submarines as a strategic deterrent," Sergei Shoigu told a meeting at the Pacific Fleet's submarine command headquarters.

The defense minister said the Pacific Fleet's submarine forces "have particular importance for ensuring strategic stability and Russia's military security in the Far East."

The meeting focused on developing the infrastructure of the nuclear-powered submarine base in view of plans to launch fourth and fifth-generation submarines.

http://en.rian.ru/military_news/20130327/180277186/Russia-to-Equip-Submarine-Forces-With-High-Precision-Weapons.html

(Return to Articles and Documents List)

The London Daily Telegraph – U.K.

Biological Attacks 'Getting Easier for Terrorists'

Terrorists will find it increasingly easy to launch attacks using biological weapons, a senior security official has warned.
By James Kirkup, Deputy Political Editor
26 March 2013

Charles Farr, the Director of the Office for Security and Counter-Terrorism, said that extremists have ever greater access to the information and technology required to create and spread germ agents or other biological weapons.

He spoke as an official assessment suggested that countering the threat to the UK from international terrorism is becoming harder and more expensive.

The Home Office has published an annual report on its Contest counter-terrorism strategy, which warned that Islamic terrorist threats are now spread more widely across the world, requiring "very significant resources" to combat.

The report showed that security officials and intelligence agencies believe that a priority for Britain is improving its ability to detect biological attacks, treat victims and decontaminate attack sites.

"Biological will get easier from a terrorist point of view," Mr. Farr said.

Factors facilitating such attacks include the availability of formulae and other information on the internet; increasing teaching of biological sciences at universities, and "greater availability of technology," he said.

Mr Farr, a former MI6 officer, declined to give further details of the threat, but the Home Office report hints at a range of new precautions.

Last year, the Home Office began enforcing a new list of controlled biological agents to "ensure that dangerous pathogens and toxins that are required in important medical and scientific research are used and held securely."

Lessons learned from the security operations for the London Olympic Games have "informed the wider programme of planning for high impact biological attacks," the report said.

The Home Office report also said that British authorities continue to plan for a Mumbai-style attack by terrorist gunmen.

In particular, the emergency services have been working on plans to treat and extract casualties from an attack scene even while violence continues.

Details are secret, but it is believed that special teams of armed police officers and volunteer paramedics have been trained to operate under fire.

Mr Farr also revealed that even as officials prepare for such attacks, the counter-terrorism budget is coming under pressure to make cuts.

Security and intelligence agencies are having to "find savings" to fund the battle against al-Qaeda, he said. In some cases, that means reducing manpower.

The warnings about the money available for counter-terrorism come as ministers discuss a Spending Review that is likely to impose more cuts on the Home Office budget after the next general election.

Danny Alexander, the Chief Secretary to the Treasury, told the Daily Telegraph last week that the Home Office could not be spared cuts in the 2015/16 round.

The Home Office report on British counter-terrorism warned that the UK faces a more complicated and widespread threat, which is more costly to address.

"The terrorist threats we face are now more diverse than before, dispersed across a wider geographical areas, and often in countries without effective governance," it said.

"This poses significant challenges to our national security and to the security and intelligence agencies and departments working on counter-terrorism: operating in these areas is difficult and dangerous, requires very significant resources and is complicated and at times made impossible by the breakdown of governance and law and order."

Mr Farr said that the changing nature of the threat puts new financial pressure on the Home Office and other agencies.

"It takes more to do the same amount of counter-terrorism work," he said. "We have to find savings."

He added: "Across the whole of the CT budget, which is in the region of £1 billion, you would expect to find some efficiency savings. Technology means that in some areas, you can do the same with fewer people."

The Home Office report also warned that British Muslims fighting in Syria's civil war could return home to carry out terrorist attacks.

http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9955007/Biological-attacks-getting-easier-for-terrorists.html

(Return to Articles and Documents List)

USA TODAY

Reports Warn of Lax Inspections, Bioterror Lab Risks

Two new government reports raise concerns about the risks posed by labs experimenting with dangerous germs that have the potential to be used as bioterror weapons.

USAF COUNTERPROLIFERATION CENTER
CPC OUTREACH JOURNAL
MAXWELL AFB, ALABAMA

By Alison Young, *USA TODAY*
March 25, 2013

The United States is at increased risk for accidents at laboratories conducting research on potential bioterror germs, such as anthrax, because federal officials have failed to develop national standards for lab design, construction and operation, according to a report to be released Monday by the Government Accountability Office. The GAO called for the standards more than three years ago.

Meanwhile, another recent government audit has found significant failures by federal officials to detect security and safety violations during inspections of bioterror labs. The undetected issues included the transfer of anthrax and plague to an unauthorized facility, and allowing workers at multiple research facilities to remain on the job with expired security risk assessments.

"As a result, there is increased risk of the misuse of select agents and the potential for serious security violations going undetected," says the November 2012 report by inspector general auditors at the U.S. Department of Agriculture.

Security at bioterror labs has been an issue of particular concern since the 2001 anthrax letter attacks that killed five and sickened 17; a scientist at an Army biodefense lab was later implicated.

USDA inspection program officials disputed many of the auditors' findings, called the report's language "unduly alarming," and refused to adopt many of the auditors' recommendations, the report says.

Officials in USDA's Animal and Plant Health Inspection Service declined to be interviewed. In a statement issued Friday, spokeswoman Lyndsay Cole said that in January the inspection program agreed to take actions to address all of the auditors' concerns. Cole said "our inspections are effective at identifying deficiencies."

The USDA and the Centers for Disease Control and Prevention (CDC) share responsibility for inspecting numerous individual labs at about 350 government, academic and commercial organizations registered to work with dangerous germs and toxins that have bioterror potential.

The USDA was put in charge of inspecting labs operated by the CDC last summer, in the wake of USA TODAY's reports about safety and security problems at CDC labs in Atlanta.

U.S. Rep. Fred Upton, chairman of the House Committee on Energy and Commerce, called the USDA inspector general's findings "very troubling" and said they show the need for oversight. He said the committee will be investigating.

"The inadequate and lax inspection practices of USDA raise additional concerns about their ability and independence to conduct effective inspections of CDC's labs to ensure safety," said Upton, R-Mich.

U.S. Rep. Henry Waxman of California, the committee's ranking Democrat, said: "It is troubling that safety and security risks that were identified years ago have still not been fixed, and that the USDA IG has identified additional new vulnerabilities."

Safety experts also expressed concerns.

Najmedin Meshkati, an engineering professor at the University of Southern California, said the USDA lab inspection program "may be suffering from a serious safety-culture problem," based on his quick review of the audit report.

Richard Ebright, a biosafety expert at Rutgers university in New Jersey, said the repeated failures by USDA inspectors to detect problems is "significant" and it "erodes confidence" that regulations are being effectively monitored and enforced. Ebright noted that the USDA "rebuffed" auditors' recommendations. "This is one of the most striking parts of the report," he said.

CDC officials declined to be interviewed or to discuss audits of their inspection program. In a statement, the CDC said: "The record stands for itself," noting that the agency has performed more than 1,500 inspections over the past 10

years. "The public should be confident that the critical research and development work to treat and prevent disease associated with select agents in the U.S. is done in a safe and secure manner."

The USDA generally oversees about 50 organizations with labs that work with pathogens that primarily pose a risk to livestock and crops, and the CDC has primary responsibility for inspecting those at about 300 entities that work with germs that are dangerous to people.

It's unclear what government auditors have found recently in similar audits of the effectiveness of CDC's inspection program. The CDC is audited by the U.S. Department of Health and Human Services inspector general, which is still processing USA TODAY's Freedom of Information Act request for the reports.

Incidents involving bioterror agents are rare, according to a CDC report last year in the journal *Applied Biosafety*. Between 2004 and 2010, there were no reports of thefts and only one confirmed loss, which occurred during the shipment of a fungus that can cause a type of pneumonia called Valley Fever. An FBI investigation of the lost fungus package concluded it was "apparently destroyed during processing at a commercial shipping facility," the CDC researchers' article said.

The CDC report said there were 11 laboratory-acquired infections among 639 potential release incidents reported to the agency during those years among more than 10,000 people with approved access at organizations working with "select agents," the government's term for germs and toxins that have the potential to be used as bioweapons. None of the infections was fatal or involved the disease spreading to others.

USA TODAY reported last month that the HHS inspector general has repeatedly cited the CDC for safety and security problems in the operation of its own labs in Atlanta and Fort Collins, Colo., including failing to secure potential bioterror agents and not properly training employees who work with them. At the time of those reports, issued in 2008 through 2010, the CDC was responsible for inspecting its own labs.

CDC officials have said nobody has been endangered by the lapses because their labs have redundant layers of safety and security to protect employees and the public. When issues arise, they are fixed immediately, the agency says.

Other incidents have also caused concern, including power outages at CDC labs in Atlanta in 2007 and 2008. In 2007, a leaky drainage system was suspected in the release of foot-and-mouth disease virus — a highly infectious livestock disease that can have significant economic consequences — from a vaccine research facility in the United Kingdom and an outbreak on nearby farms, according to the GAO, the investigative arm of Congress.

In 2009, the GAO examined the potential risks posed by the proliferation of "high-containment labs" experimenting with dangerous germs, including bioterror agents, in the wake of the 2001 terrorist attacks and increased biodefense funding. The labs' research focuses on such things as developing treatments, vaccines, diagnostic tests and other countermeasures. The GAO concluded that a national oversight strategy was needed, including a periodic assessment of the nation's need for the labs. The report also said national construction, operation and maintenance standards were needed.

But federal security and science officials in the Executive Office of the President have not acted on the recommendations, the GAO said in its new report scheduled to be released Monday. "There is still no one agency or group that knows the nation's need for all U.S. high-containment laboratories," the report said, noting that budget constraints make the need for a national strategy and prioritization "more critical today than 3years ago."

The GAO said it remains concerned that there continue to be no national standards for lab design, construction and operation. "This will make it difficult to be able to assess and guarantee safety," the report said.

According to the report, officials in the president's Office of Science and Technology Policy disagreed with the GAO's conclusion that there is an increased risk associated with the increased number of labs and said several actions have been taken since 2009 to strengthen lab security, including the creation of new regulations and committees focused on managing risks. White House officials did not respond to USA TODAY's requests for interviews or comment.

Upton said the lack of action is "not acceptable" and that the "GAO recommendations merit action and engagement by the administration."

http://www.usatoday.com/story/news/nation/2013/03/25/report-cite-increased-bioterror-lab-risks/2011007/

(Return to Articles and Documents List)

The Hill
DEFCON Hill

Hagel might have Final Say on Controversial Missile Defense Program

By Jeremy Herb
March 26, 2013

Congress appears to be ceding the decision over whether to fund a controversial $400 million missile defense program to Defense Secretary Chuck Hagel and the Pentagon's lawyers.

The Medium Extended Air Defense System (MEADS) has long been in Congress's crosshairs, and the 2013 National Defense Authorization Act (NDAA) prohibited funding the program.

But the continuing resolution that President Obama signed on Tuesday included $380 million for the program to either fund the final year of development or cover termination costs.

That throws the fate of the missile defense program — a joint venture between the U.S., Italy and Germany — into doubt, congressional aides say, as contradicting interpretations of the two measures will likely mean the Defense Department has the final say.

Pentagon officials aren't tipping their hand yet.

On Tuesday morning, spokeswoman Lt. Col. Melinda Morgan said it would be "premature" to discuss the measure because it was not yet signed by the president. She did not respond to a request for comment after the bill was signed by Obama in the afternoon.

Officials at Lockheed Martin, the main U.S. contractor for MEADS International, say they are expecting the money will be used to fund the program in 2013, although the company has not yet received any guidance from the Pentagon.

"Clearly we were very pleased when Congress passed the FY13 omnibus," Marty Coyne, director of business development for MEADS International, told The Hill.

"We haven't been told anything yet, but we're optimistic that we'll be authorized those funds to complete the development."

MEADS was intended more than a decade ago to replace Raytheon's Patriot Missile system. The Army decided in 2011 it was not going to put the system into operation, but it still wanted to complete the project's "proof of concept" development for the technology and to fulfill obligations to Italy and Germany.

Raytheon and Lockheed Martin have engaged in an intense lobbying battle over MEADS as lawmakers have attempted to kill the project, industry sources say.

Sen. Kelly Ayotte (R-N.H.) lambasted the program last week as the "missile to nowhere," as she launched an unsuccessful attempt on the Senate floor to remove funding from the appropriations bill. Her amendment was not allowed a vote.

Her nonbinding amendment to eliminate funding for MEADS was included in the Senate's 2014 budget resolution, which passed 94-5.

Sen. Dick Durbin (D-Ill.), the Senate Defense Appropriations subcommittee chairman, argued on the floor that the costs of terminating the program were roughly equal to the costs to finish development, because the U.S. would have to pay Italy and Germany for breaking its contract. Thus, the Pentagon might as well fund the program, he said.

MEADS is funded by unused 2012 funds through the end of March, meaning the Pentagon will likely need to make a decision soon on what to do in 2013.

DOD won't get much help from Congress. The congressional committees that handle defense issues disagree over what the Pentagon can do with the $380 million it's been given for MEADS.

House appropriators say that the NDAA has precedent because it sets Pentagon policy, and therefore the money can only cover termination costs. Appropriations Committee Chairman Hal Rogers (R-Ky.) made a point of stating that during debate on the House floor earlier this month.

But Senate appropriators argue the CR gives the Pentagon discretion. An aide to Senate Defense Appropriations ranking member Richard Shelby (R-Ala.) — one of five senators to vote against Ayotte's budget amendment — said the appropriations bill has precedent because it was the latest measure passed by Congress.

Even the Armed Services Committees, which initially passed the prohibition on funding MEADS, are split.

A House Armed Services aide said that the funding tables in the CR were made "binding," which means they are considered legislative language and have equal weight as the authorization bill provision that banned funding for the medium-range missile program.

But a Senate Armed Services aide said the appropriators could not overrule the prohibition.

"That provision is in the law and DOD has to abide by law — they're not going to ignore the fact that this is the law, even if there's money in CR-Appropriations bill," the aide said.

http://thehill.com/blogs/defcon-hill/army/290433-pentagon-may-have-final-say-on-controversial-missile-defense-funds

(Return to Articles and Documents List)

Defense News.com

Cyber Threats Can Lurk in DoD Electronics, Software Purchases

March 26, 2013
By DEBRA WERNER

When Scott Borg began warning a decade ago of the various ways adversaries could infiltrate electronic supply chains, the danger was largely theoretical. He suggested that an adversary might embed malicious programs in microcircuitry, and then spy on or sabotage weapons and other electronic equipment.

"When my colleagues and I first talked about these things, the actual evidence we could point to was slender and patchy," said Borg, director of the nonprofit U.S. Cyber Consequences Unit. "It was persuasive if you took the time to study it, but not if you had to cite it quickly to a skeptical audience."

A decade later, audiences are no longer skeptical. In his Worldwide Threat Assessment in March, Director of National Intelligence James Clapper listed "Threats to US Government Supply Chains," as a top concern and warned of "potential supply chain subversions." The Defense Department spends billions of dollars annually to fend off cyber attacks, yet the challenge of securing weapon and information systems is more daunting than ever.

That's due in part to the massive number of companies involved in military supply chains.

"In an era of globalized commerce, an emerging threat that concerns the Department involves possible foreign compromise of our supply chain, which could degrade or defeat our information systems or weapons platforms by

inserting malicious code or otherwise corrupting key components bound for these important war-fighting systems," Ronald Burgess, the retired Army lieutenant general who was running the Defense Intelligence Agency, told members of the Senate Armed Services Committee in February 2012.

DoD has taken that warning seriously. On Nov. 5, Teresa Takai, the department's chief information officer, and Frank Kendall, undersecretary for acquisition, technology and logistics, issued policies designed to minimize the risk that "foreign intelligence, terrorists, or other hostile elements" could sabotage or subvert critical systems or components. The new policies direct DoD officials to carefully evaluate individual vendors, particularly the ones who supply code or components of critical systems. They also instruct program managers to conduct rigorous testing and evaluation to identify vulnerabilities in hardware and software.

In December, the Defense Advanced Research Projects Agency launched its own campaign to improve security for information technology. Through the Vetting Commodity IT Software and Firmware program, DARPA is challenging companies to come up with innovative ways to uncover the type of malicious instructions adversaries could use to steal data or sabotage critical operations.

"Determining the security of every device DoD uses in a timely fashion is beyond current capabilities," an agency announcement said Dec. 19.

While cybersecurity experts applaud the Pentagon's recent initiatives, they warn that the threat of enemies tampering with hardware, software or data spread through computer networks and mobile devices continues to grow. An enemy could, for example, design malware for a missile system that would lie dormant until the weapon was set for launch and then substitute new geopositioning coordinates for the intended target. This type of attack would be extremely costly and difficult to accomplish, but the stakes are too high to ignore the risk, Borg said.

What's more, cyber threats have become far more complex in the last decade.

"We see organized crime and nation states becoming more patient and thinking through attacks," said Gib Sorebo, SAIC vice president and chief cybersecurity technologist. "Just like in spy movies, when James Bond had to get into one facility to get information to get into another facility, we are seeing cyber attacks that are multifaceted and they are targeting suppliers because oftentimes suppliers are easier to attack and oftentimes people don't suspect them."

The creators of Flame, sophisticated code that spread undetected among computers in the Middle East from 2010 to 2012, used forged Microsoft Windows licensing certificates to spread the malware through fraudulent Windows updates. Hackers also used two-factor authentication tokens stolen from EMC's RSA Security Division to break into Lockheed Martin networks in 2011.

There's no simple way to prevent these attacks. Weapon systems are jam-packed with software and electronic components. Each component is laden with circuitry. Computer experts often have trouble identifying the precise job of each circuit.

"Even if people went to the trouble of attempting to verify that every chip on a circuit board came from a reputable supplier and nothing untoward had been put on there, which virtually no one does, they would still need to make sure the exemplar they were using had not been compromised," Sorebo said. "We are just beginning to figure out ways to solve the problem."

TRUST IN THE CLOUD

Still, there are obvious steps companies and government agencies can take to improve security, including figuring out who has access to critical data. With the growing use of cloud computing and mobile devices, data that was once held by a single organization is now shared among many. In a recent survey, one multinational corporation discovered that its data was stored in 15 to 20 different places, said Steve Durbin, global vice president for the nonprofit Information Security Forum, an organization that considers supply chain security among the five top threats to businesses in 2013. Within any enterprise, it's important to understand what information is being shared, where that information is being stored, how it is being stored and who has access to it, Durbin added.

Similarly, companies and government agencies should evaluate the safety and security of their global hardware and software supply chains.

“If you look at the hardware you buy, virtually none of it is manufactured by the actual company with its name on it,” Sorebo said. So it’s not simply a question of trusting Dell or Cisco, but of trusting every supplier those companies rely on, including companies that provide cloud-based computing services, he added.

In October, a U.S. House Intelligence Committee report raised concerns that China’s Huawei Technologies Co. and ZTE Corp. could not be trusted to provide telecommunications equipment, components or services for U.S. government programs or U.S. government contractors because of the close relationships those companies have with the Chinese government. Some security experts also have raised concerns about the world’s most rapidly growing semiconductor company, GlobalFoundries, based in the United Arab Emirates. GlobalFoundries, which was established in 2009, is the world’s second largest semiconductor fabrication plant that specializes in producing the chips its customers design.

In spite of concerns that hardware and software created in China or the Middle East pose greater risk than domestic products, security experts reject suggestions that the Pentagon limit its procurement to electronic components built in the United States or take pains to identify the country of origin for individual parts. Those exercises would be “prohibitively expensive and infeasible, based on the mechanisms that are currently readily available,” representatives of the CIA and the Office of the Director of National Intelligence told the Government Accountability Office, according to the report, “IT Supply Chain: National Security-Related Agencies Need to Better Address Risks,” published in March 2012.

The military reaps enormous cost and performance advantages from its access to global suppliers. Cybersecurity experts said any steps the government takes to improve security should not prevent that access or include such heavy reporting or due-diligence measures that those cost savings disappear. Instead, government agencies and companies should institute common-sense security measures for all programs, such as vetting suppliers and evaluating whether those suppliers conduct background checks on managers and employees.

Additional security measures are likely to vary from program to program. For weapons critical to national security or those in which a malfunctioning component could cause grave harm, stringent security precautions are warranted. In secure facilities program managers may be restricted to using parts produced domestically.

“It’s similar to the way we treat classified information, with checks at each level of the supply chain,” Sorebo said.

Still, those procedures will increase the cost of products and services, so they should only be employed when a particular program is considered high risk. He said DoD will want to use different procedures to ensure the safety of tires purchased by the Defense Logistics Agency than it would to safeguard infrastructure designed to support the nation’s response to nuclear attack.

In addition, security precautions will vary even among high-risk programs.

“We can’t just think about cybersecurity in terms of patching and avoiding vulnerabilities,” Borg said. “We have to think about threats, consequences and the total risk picture.”

Military leaders should look at an individual weapon, for example, to determine who would want to attack it, what kind of attack they would want to carry out and what harm it would cause.

Once that process is completed, program managers will be in a position to implement defensive strategies. They will know, for example, which systems should be air-gapped, or insulated from any contact with the Internet. They also will know what types of anomalous behavior could signal a serious problem and how to identify that behavior. When that analysis is completed, Pentagon planners will be able to focus resources on securing the most critical systems. For many programs, basic security strategies will be adequate because cyber attacks that degrade or destroy systems would be inconvenient but not dangerous.

The Internet Security Alliance is preparing to release a lengthy set of guidelines for safeguarding the electronic equipment supply chain. These guidelines, written by Borg, are the product of a lengthy series of workshops, discussions, and interviews conducted since 2007. The guidelines will include detailed steps that manufacturers can take to secure each stage of the electronic production process, from design through fabrication, assembly, distribution and maintenance. The new guidelines also will highlight the danger posed by counterfeit electronics.

COUNTERFEIT THREATS

The Semiconductor Industry Association has issued repeated warnings about the danger of counterfeit electronics in military systems. Because the military services tend to rely on electronic equipment far longer than commercial customers, many of the components the military needs to maintain systems are no longer available from the original manufacturer.

"The Defense Department is wedded to very old technology," said a semiconductor industry executive who asked not to be identified. As a result, military procurement officers who use the Internet to search for replacement parts often end up with chips stripped from old machinery, cleaned and relabeled.

In many cases, the second-hand parts cause military systems to fail or malfunction because they are damaged, old or incorrectly labeled. However, counterfeit parts also could carry malicious firmware.

"It's possible to introduce malicious firmware into a process that is to some degree being supervised and visited by a legitimate chipmaker," Borg said. It would be much easier, however, to introduce malicious firmware on a counterfeit. "You can do things that would be hard to do subtly or covertly in another kind of supply chain," he added.

To stop counterfeit electronics from entering the U.S., the members of the Semiconductor Industry Association have lobbied for years in support of legislation that would give Customs and Border Protection agents authority to inspect suspicious packages and exchange identifying information with the purported manufacturer to confirm the authenticity of electronic devices. That was the practice until 2008, when customs agents routinely photographed chips and shared images with the manufacturer whose trademark appeared on the label to confirm the authenticity of electronic devices. In 2008, however, the Treasury Department instructed customs agents to redact identifying marks before sharing images.

Late last year, legislation designed to resume the practice of sharing identifying information appeared headed for passage but collapsed amid year-end wrangling over federal spending cuts. On Jan. 11, U.S. Reps. Ted Poe, R-Texas, and Zoe Lofgren, D-Calif., introduced legislation to once again give Customs and Border Protection agents authority to exchange detailed imagery with manufacturers.

"We are hoping a companion bill will be introduced in the Senate," said Patrick Wilson, Semiconductor Industry Association director of government affairs.

This article appears in the April issue of C4ISR Journal.

http://www.defensenews.com/article/20130326/C4ISR02/303260021/-1/7daysarchives/Cyber-Threats-Can-Lurk-DoD-Electronics-Software-Purchases

(Return to Articles and Documents List)

South China Morning Post – Hong Kong, China

US Jails Chinese Engineer for Taking Files on Missile Guidance System to China

Liu Sixing, who took to China thousands of defence firm's files on satellite-free missile guidance system, gets nearly 6 years in prison

Wednesday, 27 March, 2013

The Washington Post in Newark, United States

Measured in millimetres, the tiny device was designed to allow drones, missiles and rockets to hit targets without satellite guidance. An advanced version was being developed secretly for the United States military by a small firm and L-3 Communications, a major defence contractor.

On Monday, Liu Sixing, a Chinese citizen who worked at L-3's space and navigation division, was given a jail term of five years and 10 months by a US federal court for taking thousands of files about the device, called a disk resonator gyroscope, and other defence systems to China in violation of a US arms embargo.

The case illustrates what the FBI calls a growing "insider threat" that has not drawn as much attention as Chinese cyber operations. But US authorities warn that this type of espionage can be just as damaging to national security and US business.

"The reason this technology is on the State Department munitions list, and controlled … is it can navigate, control and position missiles, aircraft, drones, bombs, lasers and targets very accurately," said David Smukowski, president of Sensors in Motion, the small firm developing the technology with L-3. "While it saves lives, it can also be very strategic. It is rocket science."

In the past four years, nearly 100 individual or corporate defendants have been charged by the US Justice Department with stealing trade secrets or classified information for Chinese entities or exporting military or dual-use technology to China, according to court records.

"America is a global leader in the development of military technologies and, as such, it has become a leading target for the theft and illicit transfer of such technologies," said John Carlin, acting assistant attorney general for national security. "These schemes represent a threat to our national security. The intelligence community has assessed China to be among the most aggressive collectors of sensitive US information and technologies."

Earlier this month, a Chinese citizen who worked as a contractor at Nasa's Langley Research Centre was arrested at Dulles Airport in the state of Virginia and charged with making false statements to federal agents about the laptop and phone memory card he was carrying. According to an FBI affidavit, the suspect, Bo Jiang, 31, had taken a Nasa laptop that contained sensitive information on a previous trip to China.

After the arrest, Charles Bolden, the Nasa administrator, told a House of Representatives committee that he was limiting access to Nasa for the citizens of several countries, including China, pending a full security review.

In a classic espionage case, a 59-year-old former army defence contractor in Hawaii was charged this month with passing classified information to his 27-year-old Chinese lover whom he first met at a military conference.

Frank Figliuzzi, the former head of the FBI's counterintelligence division, told Congress last year that perhaps the most important measure against the theft of proprietary information "is identifying and taking defensive measures against employees".

Liu was part of a team of L-3 engineers testing the technology created by Sensors in Motion, a pioneer in gyroscope-based navigation as well as guidance systems.

Liu made trips to China in 2009 and 2010, and each time he made several presentations on the technology he was working on without his firm's permission.

Before his second trip, Liu told his supervisor he was going on vacation to Chicago, but instead he spent more than two weeks in China, speaking at a technology conference organised by Beijing and Chinese universities, prosecutors said.

Liu was stopped on his return from China in November 2010 and eventually arrested in March 2011. After a jury trial, Liu was convicted last September of violating the Arms Export Control Act and possessing and transporting stolen trade secrets.

In court last week, Liu, a 50-year-old father of three, told the judge that he did not intend to harm the US. He said he had a message for his children: "Believe me, Daddy didn't do anything."

USAF COUNTERPROLIFERATION CENTER
CPC OUTREACH JOURNAL
MAXWELL AFB, ALABAMA

http://www.scmp.com/news/world/article/1200439/us-jails-chinese-engineer-taking-files-missile-guidance-system-china

(Return to Articles and Documents List)

International Affairs Review
OPINION/Commentary

The Threat of Nuclear Proliferation: A Response to "Thou Shalt Not Fear a Nuclear Iran"

Jennifer Caylas responds to a previous IAR article arguing a nuclear Iran should not threaten the U.S.

By Jennifer Cayias, *Contributor*
March 25, 2013

In the January 28th issue of this newsletter this year, contributor Tim Miklos touched upon the real issue of whether or not a nuclear Iran would pose a threat to the international community ("Thou Shalt Not Fear a Nuclear Iran"). That issue is, into what type of adversary would the possession of nuclear weapons transform Iran? A common fear is that if Iran crosses the "red line" and develops nuclear capabilities it will be too late to take military action against Iran. Historic evidence, however, suggests that this would not be the case. The "red line" of nuclear development is not as definitive as recent administrations assert, and has actually been crossed several times over the past few decades.

Deterrence theory asserts that the mere possession of a nuclear arsenal protects a state by deterring would-be aggressors. One has only to look at the recent history of Russia, India, Pakistan, and Israel to see that this is not quite accurate. What nuclear arsenals do successfully deter is nuclear attack in general, and the potential of global nuclear war. Nuclear weapons did not deter Chechnya from waging a guerrilla war against the Russian Federation, or Tibet from defying China. They have not deterred conventional attacks on Israel by Hamas, Egypt, or Syria – despite Israel's conventional attack on Syria's nuclear facilities. Nor have they deterred attacks on Indian, Pakistani, or U.S. forces (or allies) in proxy wars in Afghanistan or Kashmir.

A nuclear arsenal grants a state a stronger image of sovereignty in the eyes of the international community, not due to a new capacity to defend itself, but to the security threat any new nuclear power poses as a potential proliferator. Ironically, what is most threatening about a nuclear Iran is not the military threat it would pose to its neighbors, nor a domino effect it might have on other Middle Eastern states' nuclear efforts.

A nuclear Iran presents expanded potential for proliferation – overt, covert, and unintentional. First, while latent and "second-tier" nuclear proliferation is already a problem without Iran's contribution, its participation in the nuclear black market thus far indicates it would most likely follow Pakistan's example, should it become a primary source. Second, a proliferation threat posed by the emergence of any new nuclear power is the possibility that such a state could follow a path similar to that of the Soviet Union – that being the fall of the regime and the destabilization of its internal security and infrastructure.

After the fall of the Soviet Union, its former territory became a haven for black market activity, including the illicit sale and trafficking of nuclear materials, to unknown and unaccountable recipients. The economic and political chaos of the 1990s particularly impacted Russia's "nuclear cities," which thrived on the nuclear facilities around which they were built. In other words, the potential threat posed by a new nuclear power is not so much the mere possession of its arsenal, but the stability (or lack thereof) of its regime and security infrastructure, and to what extent it can remain accountable for its nuclear technology.

Having a nuclear arsenal makes the stability and integrity of a state more important to the international community, precisely because of the potential threat its disintegration would pose. Since 1991, the United States and the International Atomic Energy Association (along with several non-governmental organizations) have worked to establish greater control and oversight of Russia's nuclear arsenal and facilities, with incomplete and inconsistent success. In part this is due to the limitations posed by sovereignty – Russia is deeply suspicious of foreign intervention within its

territory and unlikely to voluntarily halt a defense program it sees as invaluable to its national security. Likewise, Pakistan refused to take direct action against A.Q. Khan, when his network was exposed in 2004, for the same reasons. The threat posed by each of these states is not that they might use their arsenals, but that they do not have complete control over them.

Last year, Soviet and Russian scholar Kenneth Waltz argued that Iran should be given the bomb, in addition to other powers wishing to acquire it, as such a possession would place all states on common ground and reduce tensions by essentially transforming nuclear weapons into a more "conventional" weapon ("Why Iran Should Get the Bomb"). While wanton proliferation of nuclear technology cannot conceivably improve global nuclear security, the degree of proliferation that currently exists in the world validates the argument that quantity has become irrelevant – what now matters is the accountability of such weapons and of the means to make them.

In the post-Soviet world the rules of the nuclear game have irrevocably changed – deterrence no longer applies, and with technology, communication, and transportation advances prohibition has only driven proliferation underground. Therefore, the international community, starting with the United States, should change the game. More accessible and, importantly, regulated proliferation might be more effective at bringing rogue states in line than demonizing and sanctioning them.

Jennifer Cayias is a first-year graduate student at the American Military University, earning a Master's of Arts in Intelligence Studies. She received her bachelor's degrees at the University of Utah in Political Science and International Studies, and minored in Russian. Her region of focus is the former Soviet sphere, particularly Russia and the Caucasus, and Turkey.

http://www.iar-gwu.org/node/477

(Return to Articles and Documents List)

Foreign Policy
OPINION/Article

Think Again: North Korea

North Korea is a lot more dangerous than you think, but that doesn't mean that Kim Jong Un is insane.
BY DAVID KANG and VICTOR CHA
March 25, 2013

"North Korea's not that dangerous."

Wrong. There is no threat of war on the Korean peninsula because the United States and South Korea have deterred the regime for over six decades, or so the thinking goes. And the occasional provocation from Pyongyang -- full of sound and fury -- usually ends with it blowing up in its face, signifying nothing. So why worry? Two reasons. First, North Korea has a penchant for testing new South Korean presidents. A new one was just inaugurated in February, and since 1992, the North has welcomed these five new leaders by disturbing the peace. Whether in the form of missile launches, submarine incursions, or naval clashes, these North Korean provocations were met by each newly elected South Korean president with patience rather than pique.

The difference today is that South Korea is no longer turning the other cheek. After the North blew up the South Korean navy ship the *Cheonan*, killing 46 sailors in 2010, Seoul re-wrote the rules of military engagement. It has lost patience and will respond kinetically to any provocation, which could escalate into a larger conflict. Second, North Korea crossed a major technology threshold in December, when it successfully launched a satellite into orbit. Though the satellite later malfunctioned, the North managed to put the payload into orbit with ballistic missile launch technology that is clearly designed to reach the United States.

This development appears to validate former U.S. Defense Secretary Bob Gates's January 2011 claim that the regime was only five years away from fielding a missile that could threaten the continental United States. To make matters

worse, Pyongyang conducted a third nuclear test in February, which appears to have been more successful than the previous two. Within President Barack Obama's second term in office, North Korea could well be the third nation (after Russia and China) to field a nuclear-tipped ballistic missile targeted at the United States. Moreover, the North has sold every weapons system it has developed to the likes of Iran, Pakistan, and Syria. That's worth losing sleep over.

But there's another point that is often overlooked: North Korea today can threaten all of South Korea and parts of Japan with its conventional missiles and its conventional military. The North can fire 500,000 rounds of artillery on Seoul in the first hour of a conflict. Stability has held for 60 years because the U.S. security alliances with South Korea and Japan make it clear to the North Korean leadership that if they attacked South Korea or Japan, they would lose both the war and their country. And, for half a century, neither side believed that the benefits of starting a major war outweighed the costs. The worry is that the new North Korean leader might not hold to the same logic, given his youth and inexperience.

"Kim Jong Un is insane."

Don't bet on it. It was easy to make fun of his father, Kim Jong Il, with his bouffant hairstyle, awkward social skills, and dislike of public events. Kim Jong Il was clearly an introvert, and an odd one at that. But most politicians are extroverts -- they love a crowd and love attention, and Kim Jong Un fits the profile: he has a pretty young wife, likes to appear in public and give speeches, he watches basketball games, and visits amusement parks. Much of his behavior may be political theater aimed at convincing his own people that the young general is comfortably in charge, but it is also a contrast with his father's ruling style. Kim Jong Il paid no attention to the public aspect of ruling, whereas his son's visibility and embrace of popular culture appears to be aimed at convincing North Koreans that changes may actually occur under him.

Authoritarian rulers don't long survive if they're truly out of touch with reality. They need to read palace politics, reward friends and punish enemies, and manage competing interests that are vying for power. Kim Jong Il lasted from 1994 until his death in December 2011 without any obvious internal challenge to his rule, a mark of his political acumen and mastery of factional politics. Although Kim Jong Un is inexperienced, he has held power for over a year and appears to have the acquiescence -- for now -- of the most powerful actors in Pyongyang.

More important than asking whether Kim Jong Un is insane is determining whether he is cautious or a risk-taker. Any major shift in North Korean foreign policy will involve enormous hazards. If Kim moves beyond the political theater of the past 60 years -- chest-thumping, name-calling, threatening to turn Seoul into a "sea of fire" -- and actually risks a major military strike against South Korea or even the United States, he is putting his own neck, as well as his country's, on the line.

Kim faces just as many risks if he meaningfully reforms domestic, economic, or social policy. Even within a totalitarian dictatorship, there are different factions, coalitions, and bureaucratic interests that will be injured by any change in the status quo. Economic reforms, for example, may ultimately help the country but will risk chaos in the markets, weaken powerful stakeholders within the vast bureaucracy, and potentially unleash rising expectations from the general public.

An adventurous Kim Jong Un may or may not be good for North Korea and its relations with the outside world. On the other hand, a cautious Kim, who simply pursues the status quo, would mean that North Korean policy will muddle along, with no real change to the frustrating, dangerous, decades-long game of brinksmanship.

"North Korea is poor because sanctions are working."

Not even close. North Korea is poor because of an outmoded economic policy and self-imposed isolation from the world. The latest round of U.N. and U.S. sanctions, implemented in March, only target the elite. They ban the export of luxury goods and clamp down on individuals and companies that are financing proliferation activities. It's safe to say that the average North Korean does not own a yacht or wear a Rolex.

Blame lies with five bad decisions North Korea has made in the management of its economy. First, in the aftermath of the Korean War, Kim Jong Un's grandfather -- President Kim Il Sung -- focused exclusively on heavy industry

development and the military while expecting the country to be self-sufficient in agriculture. In a country that only has 20 percent arable land, that was a huge mistake. Second, rather than seek technologies and innovations like the Green Revolution that helped nations like India make enormous gains in agricultural productivity in the 1960s and 1970s, the North tried to substitute longer work hours and revolutionary zeal. Given the broken infrastructure, this was like squeezing blood from a stone. Third, rather than trade with the outside world, the North went deeply into debt in the 1970s, borrowing and then defaulting on hundreds of millions of dollars in loans from European countries, which forever lost them lines of credit with any country or international financial institution. Fourth, in the 1980s and 1990s, the North undertook extremely wasteful mega-projects, building stadiums, hydropower projects, and tideland reclamation projects -- most of which failed or were never completed. Finally, after the Chinese and Soviets stopping giving aid to the North at the end of the Cold War, Pyongyang relied on humanitarian assistance as a form of income, instead of trying to fix their economy.

One could not have imagined a worse economic plan. This country has allowed an ideology that prizes autarky to dictate economic decisions rather than taking advantage of the benefits of trade, technology, or innovation -- which is why North Korea is one of the only countries in the world to have suffered a famine *after* industrialization.

"China won't let North Korea collapse."

For now. Maintaining a close relationship with Pyongyang can be very frustrating for Beijing, and Chinese support for the latest round of U.N. sanctions was a public rebuke. The Chinese leadership has consistently urged its North Korean counterparts to reform its economy, yet Pyongyang just as consistently ignores Beijing's advice. Although there is an increasingly vociferous public debate within China over what to do with its maverick neighbor, the Chinese leadership has so far continued to conclude that propping up North Korea is better than withdrawing its support.

The relationship might not be strong, but it remains. China is North Korea's major trading partner and provides most of the Hermit Kingdom's energy needs; moreover, it has never seriously implemented any of the four rounds of sanctions the U.N. has passed targeting North Korea. Although it agreed to the most recent U.N. resolution, China would actually have to substantially change its approach to Pyongyang to make the sanctions work, and it probably won't.

China has more influence over North Korea than any other country, but less influence than outsiders think. Beijing-Pyongyang relations haven't been warm ever since China normalized relations with South Korea over 20 years ago, and both sides resent the other. But Beijing has few options. Completely isolating Pyongyang and withdrawing economic and political support could lead to regime collapse, sending a flood of North Korean refugees across the border, and potentially drawing all the surrounding countries into conflict with each other -- which could see the devastating use of nuclear weapons. And China fears that any conflict, or a collapse, could put South Korean or even U.S. troops on its eastern border. As a result, Beijing -- much like Washington -- is faced with the choices of rhetorical pressure, quiet diplomacy, and mild sanctions. As long as China continues to value stability on the peninsula more than it worries about a few nuclear weapons, it will not fundamentally change its policy towards its unruly neighbor.

"Enough carrots can make North Korea give up their nukes for good."

If only it were that easy. Since Ronald Reagan's time in office, successive U.S. administrations have put forward the idea that if insecurity and relative deprivation drive North Korea's obsession with nuclear weapons, then surely the answer is for the United States and neighboring countries to guarantee a peaceful peninsula, and provide money, food, and political recognition to the regime. This has been the basis of the agreements reached with North Korea in 1994 under Bill Clinton and in 2005 under George W. Bush. From 1989 to 2010, U.S. presidents, their national security advisors, and secretaries of state have given written and verbal assurances of non-hostile intent and a willingness to engage to the North over 33 times. Pyongyang acknowledged, rejected, and ignored these assurances, all the while continuing with their nuclear and weapons programs. In fact, the record of U.S. engagement is pretty impressive. In addition to massive amounts of food, energy, and other economic assistance given over a period from 1994 to 2008, two former U.S. presidents (Clinton and Carter) have visited with the North Korean leadership to express U.S. good intentions, as have (in less formal contexts) the New York Philharmonic, Google Chairman Eric Schmidt, and of course Dennis Rodman. Presidents Clinton, Bush, and Obama have each written personal letters directly to the North Korean

leader about a willingness to make a deal. And when North Koreans have visited the United States, they have been hosted by everyone from Gov. Bill Richardson to Henry Kissinger, and been given the company of luminaries such as Paul Volcker, Winston Lord, and Bob Hormats.

Clearly, this charm offensive hasn't worked. Signing a peace treaty in advance of denuclearization would recognize and legitimize Pyongyang's nuclear status, leaving it little incentive to shed those weapons. North Koreans have said to me that a peace treaty is just a piece of paper; why would they give up their cherished nuclear program for that?

Victor Cha is senior advisor for Asia and Korea chair at CSIS and professor at Georgetown University. David C. Kang is Professor of International Relations and Business at the University of Southern California.

http://www.foreignpolicy.com/articles/2013/03/25/think_again_north_korea?page=full

(Return to Articles and Documents List)

POLITICO.com
OPINION/Opinion Contributor

Heed Ronald Reagan on Missile Defense

By REP. DOUG LAMBORN
March 26, 2013

'Our only purpose — one all people share — is to search for ways to reduce the danger of nuclear war." With those words, 30 years ago this month, President Ronald Reagan launched America's development of a missile defense system. In the speech introducing the Strategic Defense Initiative, or "Star Wars", Reagan challenged the nation's leaders to make protecting and strengthening the peace their top priority. SDI would use a combination of ground and space-based systems to protect the United States from attack by nuclear ballistic missiles.

The 30th anniversary of the SDI speech provides us with an opportunity to revisit those timeless national security concepts articulated by Reagan, assess the growing missile and nuclear proliferation risk to our national security and reinvigorate our efforts.

Interestingly, the Obama administration recently reversed course on the importance of a key part of our missile defense system and announced it will ask Congress for the authority to deploy 14 additional interceptor missiles in response to threats from North Korea. It is good to see President Barack Obama finally taking the North Korean threat seriously. When he took office, one of Obama's first actions was to put the brakes on the plan to deploy these interceptor missiles.

Reagan's Star Wars plan was based on a simple premise: "The United States does not start fights. We will never be an aggressor. We maintain our strength in order to deter and defend against aggression — to preserve freedom and peace." It is a timeless truth, we maintain peace through strength. Weakness invites aggression.

Challenges to our resolve to protect and strengthen the peace are emerging more frequently. One glaring example is North Korea, the world's leader in missile proliferation. It continues to violate U.N. Security Council resolutions by testing intercontinental ballistic missiles and nuclear weapons. Another is Iran, which has an extensive missile development program and has received support from Russia, China and North Korea. Iran reportedly could develop and test an ICBM capable of reaching the United States by 2015.

China is moving ahead with the development of a new and more capable generation of ICBMs and submarine-launched missiles, increasing its existing ability to deliver nuclear warheads to the United States and to overwhelm missile defense systems. Russia is building a variety of new ICBMs that could carry up to 15 warheads, according to reports in the Russian press.

But China and Russia are paragons of stability compared to some countries.

The U.S. and its allies must quicken the pace if we are to stay one step ahead of unstable regimes that continue to develop credible missile and nuclear capabilities with which to threaten democracies around the world.

The Missile Defense Agency continues to be highly successful in deploying U.S. capability and in forging technology partnerships with our allies. Missile defense interceptors are deployed to Alaska and California and are standing ready to provide homeland defense. We work jointly with Israel. We are collaborating with our European allies to implement the European Phased Adaptive Approach that culminates in 2021 with a system able to intercept medium and intercontinental ballistic missiles. Without adequate funding both the U.S. and our allies are at risk.

Reagan also acknowledged the budgetary challenge by reminding the nation that funding missile defense is more than an "arithmetic exercise." Today, as in 1983, many agitate for reducing our military using simple subtraction to balance the budget without fully understanding or addressing the national security consequences of such a simplistic approach. In Obama's first budget to Congress, he proposed slashing more than 10 percent from the missile defense budget in a single year. He has continued to seek even further reductions since then. For example, in the fiscal year 2010 budget, Obama canceled every missile technology development program.

The administration has yet to satisfactorily address how the nation will "protect and strengthen the peace" against missiles launched from the Middle East. Hollowing out our missile defense capability, given the increased risk to our national security, would not allow the U.S. to protect and strengthen the peace. Weakening our missile defense capability simply encourages other countries to test our resolve.

Thirty years ago this month, Reagan used his foresight and leadership to inspire the nation to accomplish the impossible by moving beyond the perceived possibilities of the day. We must once again focus the nation on the goal of protecting and strengthening the peace — attainable only from a position of strength. A lot has changed since 1983, but the need for a robust missile defense has never been greater.

Rep. Doug Lamborn (R-Colo.) is a member of the House Armed Services Committee and co-chairs the Missile Defense Caucus.

http://www.politico.com/story/2013/03/heed-reagan-on-missile-defense-89331.html

(Return to Articles and Documents List)

The Japan Times – Japan
OPINION/Commentary

Asian Pivot Key to Rebooting Nuclear Disarmament Efforts

By Richard Weitz
March 28, 2013

WASHINGTON – In 2009, U.S. President Barack Obama pledged to seek a world without nuclear weapons. While he delivered on his promise to negotiate a New Strategic Arms Reduction Treaty with Russia a year later, progress has since stalled.

To break the deadlock, the current bilateral framework for negotiation, which has remained largely unchanged since the Cold War, must be transformed into a trilateral framework that includes China.

To be sure, such a move would significantly complicate negotiations. After all, while decades of bilateral dialogue have given the United States and Russia a good sense of each other's strategic perspectives — including the issues on which they disagree — China's perception of strategic stability is unfamiliar. But trilateral dialogues, catalyzed by skillful U.S. diplomacy, could also serve as an opportunity to manage the countries' strategic relations, which are characterized by contradictions and mistrust.

Russia seeks China's support in opposing American missile-defense systems, and calls for the involvement of all nuclear states in future strategic arms-control talks, but then cites concerns about China's military modernization to justify its refusal to negotiate with NATO on tactical nuclear-weapon reduction.

China, which has never adopted legally binding limits on its nuclear weapons or strategic nuclear-delivery vehicles, rejects Russia's call to join negotiations — a stance that the U.S. supports until the Russian and U.S. nuclear arsenals move closer in size to those of China.

At the same time, U.S. officials deny that their country's missile-defense programs are directed against Russia or China, but refuse to offer a legally binding guarantee. And the U.S. Department of Defense is developing a robust program of long-range conventional strike weapons, which China and Russia cite to justify their efforts to strengthen their offensive nuclear forces.

Although multilateral cooperation on nuclear issues has been effective in some cases, such as in ratifying the Nuclear Nonproliferation Treaty, it has been inadequate in others, such as in easing tensions with Iran and North Korea. In fact, even when China, Russia and the U.S. share the same agenda, their differing diplomatic tactics often undermine their ability to achieve their objectives.

For example, the three countries' policies are inadvertently contributing to proliferation pressures in Asia and Europe. U.S. pledges to defend Japan against a nuclear attack from China or North Korea have played a decisive role in dissuading the Japanese from seeking their own nuclear weapons. Given this, a Chinese nuclear surge — even one that did not lead to U.S.-China parity — could undermine the credibility of American deterrence commitments, possibly motivating Japan to launch its own nuclear program.

Similarly, some of NATO's newer members, many of which are former Soviet-bloc states, are anxious about the prospect of Russian rearmament. As a result, they oppose efforts to reduce the number of American nuclear weapons in Europe, part of NATO's "nuclear sharing" policy.

Perhaps the biggest obstacle to initiating a trilateral dialogue is Chinese resistance to formal nuclear arms-control agreements, which is rooted in the memory of Cold War-era nonproliferation initiatives aimed partly at preventing China from developing a nuclear deterrent. Since then, Chinese officials have insisted that they do not belong in U.S.-Russian strategic-arms talks, because the two countries' nuclear arsenals dwarf theirs.

But, as the U.S. and Russia reduce their nuclear stockpiles, this excuse is becoming less valid, and China's exclusion from negotiations is becoming an increasingly significant hindrance to disarmament. Securing a binding commitment from China's government to limit its nuclear development is crucial to reassuring the U.S. and Russia that further strategic-weapons cuts will not undermine global or regional stability.

Several recent developments could help to minimize obstacles to trilateral cooperation. China's new leadership is further removed from Maoist-era reflexive opposition to nuclear negotiations; Russian leaders' confidence in their economic and military resurgence is waning; and both countries are increasingly frustrated by the lack of progress in nuclear talks with North Korea and Iran. Meanwhile, faced with a large federal budget deficit, many American voters would welcome reduced spending on nuclear weapons.

The U.S. should capitalize on this situation, leveraging Russian concerns and interests to induce China to join strategic arms-control efforts. China might be willing to make a unilateral, but enforceable, commitment not to augment its nuclear arsenal, if Russia and the U.S. reduce theirs further. Determining the circumstances that might induce such restraint — and the conditions that would be needed to sustain it — is crucial to reinvigorating nuclear disarmament efforts.

With Russia ostensibly on board, it is up to the U.S. to initiate a transformation in the nuclear-negotiation framework — and that means convincing China to participate.

Richard Weitz is a senior fellow and director of the Hudson Institute's Center for Political-Military Analysis. 2013 Project Syndicate

USAF COUNTERPROLIFERATION CENTER
CPC OUTREACH JOURNAL
MAXWELL AFB, ALABAMA

http://www.japantimes.co.jp/opinion/2013/03/28/commentary/asian-pivot-key-to-rebooting-nuclear-disarmament-efforts/

(Return to Articles and Documents List)

Wall Street Journal
March 28, 2013

How Iran Could Get the Bomb Overnight

Building a nuclear weapon takes time. Buying one does not.

By Edward Jay Epstein
Page - A13

The West has tried to stop Iran from manufacturing nuclear weapons by diplomacy, sanctions and cybersabotage, and with the threat of military action if Tehran crosses red lines in moving toward the final stages of making a bomb. If Iran becomes discouraged in its efforts, an easier and more immediately dangerous option is available: buying nuclear weapons from North Korea.

When it comes to manufacturing weapons of mass destruction, the Iranian regime is in a bind. To further enrich its current stockpile of lowly-enriched uranium hexafluoride gas to weapons-grade material, Tehran would need to reconfigure its centrifuges. Since those centrifuges are closely monitored by inspectors of the International Atomic Energy Agency, Iran would have to expel the inspectors, explicitly breaking out of the Non-Proliferation Treaty.

Then it would take four to six months -- according to the head of Tel Aviv University's Institute for National Studies, Amos Yadlin -- to produce enough enriched uranium for a bomb. During this interval, Tehran would effectively invite an attack by the U.S. and Israel, which have repeatedly stated that they will not allow Iran to produce fissile fuel for weapons. Since the U.S. has munitions capable of destroying all of Iran's centrifuges above ground at Natanz and sealing off the entrances to its underground facilities at Fordo -- plus the Stealth bombers to deliver these knockout punches -- Iran would likely lose the means to manufacture nuclear weapons before it could make a single one.

But what if Iran buys one or two nuclear warheads from North Korea? The government in Pyongyang has already conducted three nuclear tests and claims that it has nuclear warheads that fit on its No Dong medium-range ballistic missiles. If that claim is true, then mounting the warheads on Iran's Shahab missiles, which are copies of the North Korean ones, would present little problem. After all, Iran has collaborated with North Korea on missile design for more than a decade.

These off-the-shelf weapons would leave virtually no window of opportunity for a pre-emptive attack by the West and its allies. The warheads could arrive in Iran on a plane in the middle of the night and be immediately fitted onto Iranian missiles. Iran would not have to actually use these missiles to have a deterrent. It could renounce the Non-Proliferation Treaty and flaunt its nukes, as North Korea has done for seven years without suffering a military attack by the U.S. Indeed, such a fait accompli would give Iran the same potential for nuclear retaliation as North Korea.

Do we know for sure that North Korea has nuclear warheads it could transfer to Iran? There is little doubt that the country has the means to produce between three and six nuclear bombs annually. In 2011, North Korea invited a former director of the Los Alamos National Laboratory, Siegfried Hecker, to inspect a state-of-the-art uranium-enrichment plant at Yongbyon, with just such a capability. According to a Feb. 13 report by the Congressional Research Service, U.S. intelligence believes that, in North Korea, "it is likely other, clandestine enrichment facilities exist" to produce fissile material for bombs.

North Korea has already demonstrated its willingness to engage in illicit nuclear proliferation by selling a nuclear reactor to Syria (the reactor was destroyed by Israeli bombers in 2007.) We also know that Pyongyang desperately needs money and that, even with sanctions, Iran has billions in oil revenue. If the price is right, then, the North Koreans have every reason to make a deal.

One ominous sign that such a deal may be in progress came in February reports by the Sunday Times of London and the Times of Israel that the Iranian physicist Mohsen Fakhrizadeh was in North Korea when it conducted its third nuclear test last month. Mr. Fakhrizadeh, one of the architects of Iran's nuclear program, reportedly headed Iran's secret "project 111," which, according to the 2007 CIA National Intelligence Estimate, worked to design warheads that could be used on Iranian missiles. If he indeed observed the test last month, it would not have been as a tourist.

By focusing on preventing Iran from manufacturing a nuke and relying on time to plan a pre-emptive strike, the U.S. may be neglecting Iran's far more dangerous option of buying the bomb. Stopping the delivery of a warheads shipment would not be easy. Not being ready to stop it could prove catastrophic.

Edward Jay Epstein is an American investigative journalist and a former political science professor at Harvard, UCLA, and MIT. Mr. Epstein's most recent book is "The Annals of Unsolved Crime" published this month by Melville House.

http://online.wsj.com/article/SB10001424127887323419104578378434011235810.html

(Return to Articles and Documents List)

Los Angeles Times
OPINION/Op-Ed

'Star Wars' Today: What would Reagan Do?

He'd make the world safer by sharing missile defenses with Russia.
By Graham Allison
March 28, 2013

President Reagan stunned fellow citizens and the world 30 years ago this month with a dramatic announcement that the United States would develop and deploy a system capable of intercepting and destroying strategic ballistic missiles. Like President Kennedy's pledge to send a man to the moon, Reagan's vision was meant to stretch minds to new realities that most found inconceivable.

As the Strategic Defense Initiative, or SDI, developed, this vision encompassed three big ideas. First, technological advances would make it possible to "hit a bullet with a bullet." Second, when fully deployed, this missile defense system would "render nuclear weapons impotent and obsolete." For Reagan, this was an essential steppingstone to his even grander vision of a world free of nuclear weapons. Third, to persuade America's Cold War adversary to eliminate its superpower nuclear arsenal as well, Reagan proposed to share this SDI technology with Moscow.

All three dimensions of Reagan's vision drew immediate, fiery criticism at home and abroad. Skeptics argued that killing a missile with a missile was technically impossible. Thirty years and more than $150 billion of investment later, this objection has been largely overcome. Today, the United States and its allies have deployed missile defense systems for shorter-range missiles (for example, the Israeli Iron Dome and U.S. Patriot systems) and for longer-range missiles (the sea-based Aegis system and a ground-based system deployed in Alaska). Just this month, in response to North Korea's threats, the Obama administration announced plans to deploy an additional 14 ground-based interceptors.

Reagan's vision of a world free of nuclear weapons was initially rejected by most of the American establishment as naive and dangerous. In the last decade, however, four of the bluest chips from the American Cold War establishment — George Shultz, Henry Kissinger, William Perry and Sam Nunn — have put this back on the American strategic agenda.

In his first international speech as president, in Prague in the spring of 2009, Barack Obama made this goal his own, arguing that the existence of nuclear weapons is "the most dangerous legacy of the Cold War." The new START arms control agreement reached by Obama and Russia's then-President Dmitry Medvedev in April 2010 took a modest step toward that end.

Perhaps the most controversial aspect of Reagan's concept was his proposal to share this technology with our Soviet adversaries. During their October 1986 summit in Reykjavik, Iceland, Reagan proposed to Soviet leader Mikhail Gorbachev "to share the benefits of strategic defense. We will agree now to a treaty committing to do so in conjunction with the elimination of ballistic missiles." Moreover, Reagan promised that it would be a "binding treaty that would provide for the sharing of research that demonstrated a potential for defensive applications."

Although Gorbachev was intrigued by Reagan's aspiration to eliminate all nuclear weapons, he and his government were suspicious of U.S. intentions. Thus, at the end of the summit, Gorbachev rejected Reagan's bold package because Washington refused to accept Moscow's condition that SDI research be confined to laboratories for a decade.

Today, the issue of ballistic missile defense remains a major stumbling block in U.S.-Russian relations, stalling both greater cooperation between the U.S. and Russia in countering Iran's nuclear ambitions and efforts to negotiate further reductions in nuclear arms. Specifically, Moscow is insisting on "binding guarantees" that U.S. missile defenses will not target or affect Russia's strategic nuclear deterrent. In reality, current U.S. missile defense systems are capable only of defending against a limited number of primitive ballistic missiles (without sophisticated decoys), and thus could not effectively defend against a Russian nuclear missile attack. Instead, the unambiguous objective of current U.S. missile deployments is to defeat Iranian and North Korean missile threats and provide protection for U.S. forces and allies against those missile programs.

At this impasse, what would Reagan do? One can be sure that he would be thinking well outside the box of conventional proposals now on the table. My bet is that he would offer the Russians not only transparency about U.S. missile defense systems, but actual shared control of those systems in a reconfigured deployment that would incorporate Russian as well as U.S. radar systems, and invite Russia to join the U.S. in deploying defenses against emerging nuclear threats. This proposal would also include major reductions in both U.S. and Russian strategic and tactical nuclear arsenals. And the prospect of serious, joint deployments that promised to neutralize the Iranian missile threat would certainly have a stunning impact in Tehran.

If Obama borrows a page from Reagan's playbook, Republicans in Washington who claim the 40th president's mantle would be shocked. But the burden would be theirs to explain why deploying missile defenses that would make the U.S. and our allies safer from attacks by Iran and North Korea is not in America's interest.

Graham Allison is director of the Belfer Center for Science and International Affairs at Harvard's Kennedy School and a former assistant secretary of Defense.

http://www.latimes.com/news/opinion/commentary/la-oe-allison-missile-defense-reagan-20130328,0,6240638.story

(Return to Articles and Documents List)

Washington Times
OPINION/Commentary

LYONS: How to Neutralize China's Military Threat

A U.S. shot across the bow could slow the dragon
By James A. Lyons
Friday, March 29, 2013

On March 14, China completed the transition of its new leader, Xi Jinping, with his assumption of the presidency. His main power comes as the leader of the Communist Party and as chairman of its Central Military Commission. While trying to project his image as a "man of the people," his various speeches on "the China Dream" have a definite military overtone, even though he professes to continue the peaceful development policies of his predecessor. He has launched a well-planned campaign to enhance the military force of the People's Liberation Army in order to give China the capability to "fight and win wars." Such statements undercut the theme that China's military buildup is only for defensive purposes.

USAF COUNTERPROLIFERATION CENTER
CPC OUTREACH JOURNAL
MAXWELL AFB, ALABAMA

China's unrelenting drive to become the dominant military power in the western Pacific continues with its just announced 10.7 percent increase to its military budget. This double-digit increase takes on added significance when viewed in light of the Obama administration's sequestration and previous, draconian budget cuts to U.S. military forces. With the continued turmoil in the Middle East, as well as Russia's efforts to revive Soviet Cold War tactics to test our readiness both militarily and politically, it is questionable whether the "strategic pivot" to the Pacific can ever be fully implemented.One of the key weaknesses of the pivot strategy is that it does not address China's development of a globally deployable military force and the establishment of nuclear and non-nuclear and proxy states, such as North Korea and Iran. As Richard Fisher, a senior fellow at the International Assessment and Strategy Center, has pointed out, such an imbalance has the potential for China to create a number of "Chinese pivots" that could quickly overstress and thus limit or deter U.S. strategy.Another element that cannot be discounted is the potential for a large Chinese nuclear breakout. China has more than 3,000 miles of underground reinforced tunnels for their fixed and mobile strategic weapons. In a Feb. 11 Wall Street Journal article by Bret Stephens, Gen. Victor Esin, former chief of staff of Russia's Strategic Rocket Forces, highlighted the "stealthy" rise of China to a position of nuclear parity with the United States and Russia. He stated that China may have 850 warheads ready to launch, and he estimated China's inventory of nuclear weapons at between 1,600 and 1,800 warheads, as compared with the current U.S. estimate of China having 200 to 400. Many reports note the administration wants to reduce U.S. warheads to 1,000 or fewer.Gen. Esin went on to state that he has solid evidence that China conducted a multiple-warhead test in July 2012, and a month later, launched a new, long-range multiple-warhead-capable missile from a submarine. Any future START talks with Russia must recognize China's nuclear inventory.Clearly, we need an immediate "shot across China's bow" that would have an impact. Putting anti-ship ballistic missiles on U.S. ships, submarines and aircraft could be just such a shot, threatening China's navy to show them they will gain nothing by using their fleet against the United States and its allies. Such a capability could be accomplished in the near term as a relatively inexpensive option, while posing a risk to China's ever-expanding surface navy.

The potential impact of introducing anti-ship ballistic missiles into our naval and air forces would be significantly multiplied if we could sell such a capability to our allies, provided an agreement can be reached with Russia to retire the 1987 Intermediate Nuclear Force (INF) Treaty. This probably is feasible, since, according to Russia's Gen. Esin, if China does not stop expanding its nuclear inventory, Russia will consider abandoning the INF Treaty. Another action that we can take is to create an Asian regional long-range sensor network that would provide our allies real-time warning of broad Chinese military activity. For such a network to become a reality, we should capitalize on the recent decision to install a second Forward Based X-Band Transportable (FBX-T) radar in southern Japan by placing a similar radar in the Philippines. We currently have an FBX-T radar in Shariki, Japan, with a 600-to-1,200-mile range. Installing an updated 3,700-mile-range SBX radar in the Philippines would permit continuous missile and aircraft coverage of all nations in the western Pacific littoral, including China.Even in this tight budget climate, we should find the funding to pursue the development of energy weapons. For example, a railgun with "shotgun" pellets flying at Mach 5 has the potential to produce a "steel cloud," which would shred most missiles, cruise missiles and aircraft flying through it. In tests, the railgun has fired artillery-size projectiles up to speeds of Mach 5 with a potential range of 62 miles. Such a system would be quite adaptable to a destroyer-sized ship.Clearly, we have a number of options that can be brought to bear, including selling nuclear submarines to allies such as Australia and Japan. However, all our conventional options must be underpinned by a credible nuclear deterrent. Therefore, it is absolutely essential to modernize our nuclear-weapons inventory. To make our options a reality, the Obama administration needs to recognize China's strategic objectives and the threat they pose to our national interests and those of our allies, and institute programs that pose an unacceptable risk to China.

Retired Adm. James A. Lyons was commander in chief of the U.S. Pacific Fleet and senior U.S. military representative to the United Nations.

http://www.washingtontimes.com/news/2013/mar/29/how-to-neutralize-chinas-military-threat/

(Return to Articles and Documents List)