USAF COUNTERPROLIFERATION CENTER

CPC OUTREACH JOURNAL

Maxwell AFB, Alabama

Issue No. 848, 1 October 2010

Articles & Other Documents:

Welcome to the CPC Outreach Journal. As part of USAF Counterproliferation Center's mission to counter weapons of mass destruction through education and research, we're providing our government and civilian community a source for timely counterproliferation information. This information includes articles, papers and other documents addressing issues pertinent to US military response options for dealing with 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.

RIA Novosti – Russian Information Agency

Clinton Urges Senate to Ratify New START Treaty after Mid-Term Elections

1 October 2010

U.S. Secretary of State Hillary Clinton urged the Senate to ratify a new strategic arms reduction treaty with Russia after the November 2 mid-term elections.

"The support for new START by our entire military leadership, our intelligence community, six former secretaries of state, five former secretaries of defense, three former national security advisors, and seven former commanders of U.S. Strategic Command is an extraordinary endorsement of why this treaty needs to be passed, and passed in the lame duck session," Clinton told reporters after a meeting with John Kerry, who chairs the Senate's foreign affairs committee.

The U.S. Senate Foreign Relations Committee recommended in mid-September that the Senate ratify a new strategic arms reduction treaty with Russia signed by the U.S. and Russian presidents on April 8 in Prague as a replacement for the START 1 treaty that expired in December 2009.

"This vote that was in the committee demonstrates unequivocally that national security is a bipartisan commitment. As we have seen with every arms control agreement, going back to the original START 1 treaty that was passed, ratified by the Senate 18 years ago tomorrow, this is an obligation and responsibility that senators addressed without regard for the day-to-day politics," the U.S. secretary of state said.

U.S. President Barack Obama and other top officials also urged the Senate to speed up the ratification of the Russian-U.S. pact.

The agreement is yet to be ratified by both chambers of the Russian parliament and the U.S. Sentate. The Russian and U.S. presidents earlier agreed that the ratification processes should be go ahead side-by-side.

The Democrats currently control just 59 seats in the upper house of the U.S. Congress, while a total of 67 votes are needed to ratify the agreement.

Clinton thanked Kerry and Republican Senator Richard Lugar for being "at the forefront of making the case why the treaty is so much in America's national security interests."

"I thank the chairman for his leadership, for the great vote that we got from the committee, and I look forward to the vote in the lame duck session that will once again demonstrate the Senate joining all of its predecessors in years past to continue to support arms control treaty," she said.

WASHINGTON, October 1 (RIA Novosti)

http://en.rian.ru/mlitary_news/20101001/160784738.html

(Return to Articles and Documents List)

Bloomberg Businessweek

U.S.-Russia Accord on Missile Defense Almost Ready, Lavrov Says

October 01, 2010

By Lucian Kim

Oct. 1 (Bloomberg) -- Russian Foreign Minister Sergei Lavrov said the U.S. and Russia are close to reaching an agreement on missile defense, the “hot potato” issue that has held up a new arms control accord between the two countries.

Presidents Barack Obama and Dmitry Medvedev, who last met in June, agreed to come up with a joint expert review on the risks of missile proliferation, Lavrov said today in an interview published in Rossiiskaya Gazeta, the Russian government’s official newspaper.

“The paper should be ready soon,” Lavrov said. The next step will then be to examine common responses, together with the Europeans, beginning with diplomacy and not excluding military force, the foreign minister said.

U.S. missile defense plans were a cause for the deterioration of relations under former President George W. Bush, and Senate opposition to a new nuclear arms-reduction treaty centers on concern the treaty will cripple America’s ability to develop a missile shield. The Obama administration has dismissed the criticism as unfounded as it seeks to win greater Russian cooperation on Iran and Afghanistan.

While Lavrov said missile defense remains a “hot potato,” he praised the improvement in ties since the Obama administration called for a “reset” in relations last year.

Rapprochement

Russia has welcomed the rapprochement, avoiding a harsh reaction to a summer spy scandal, in which 10 alleged Russian agents were deported from the U.S., and glossing over Secretary of State Hillary Clinton’s reiteration in July of plans to speed up a missile defense system in Poland. Russian Defense Minister Anatoly Serdyukov paid his first visit to the Pentagon in September, pledging closer cooperation with his U.S. counterpart Robert Gates.

“You need to present your positions in talks, not through the microphone as was so often the case with the previous administration,” said Lavrov. “The more we strengthen the fabric of our trade, investment and innovation relations, the firmer the Russian-American partnership will become.”

Medvedev, who is seeking American experience and capital to build a Russian “Silicon Valley” outside Moscow, has been willing to support U.S. policies on Iran and Afghanistan in return. Russia’s support for tighter UN sanctions against Iran because of its nuclear program this summer was “not an isolated action,” Lavrov said.

“I think Iran clearly heard the opinion of the international community,” said Lavrov, adding there’s “reason to believe” that Iran will soon return to talks in the “P5 Plus One” format including the U.S., U.K., France, Russia, China and Germany.

Editors: Patrick G. Henry, Chris Kirkham

http://www.businessweek.com/news/2010-10-01/u-s-russia-accord-on-missile-defense-almost-ready-lavrov-says.html

(Return to Articles and Documents List)

YahooNews.com

Iran Nuclear Plant Hit by Two-Month Delay: Official

By Agence France-Presse (AFP)
29 September 2010

TEHRAN (AFP) – Iran's atomic chief said on Wednesday that the country's first nuclear power plant will be ready to generate electricity by January -- two months later than announced.

Ali Akbar Salehi said that the process of placing fuel rods at the Bushehr facility, built by Russia, would be completed by the "middle of" the Iranian month of Aban, around November 7, the state television's website reported.

"Two or three months from then, the electricity generated by the plant will be connected to the grid," said Salehi, chief of Iran's Atomic Energy Organisation.

Iran began loading the Russian-supplied fuel rods on August 21 and Ali Shirzadian, spokesman for the atomic body, had then said the plant would be connected to the national grid by end of October or early November.

But Salehi later had said that the loading would begin at the end of the Iranian month of Shahrivar (September 22) and by the end of the month of Mehr (October 22), the lid of the reactor would be shut.

Salehi, in an interview with Al-Alam television on August 31, blamed the delays on Bushehr's "severe hot weather" and safety concerns, adding that the loading was being done during the night.

Iran has not hinted at any other reasons for the delay, but officials have acknowledged that a computer worm is mutating and wreaking havoc on computerised industrial equipment in the country, where an official said on Monday that about 30,000 IP addresses had already been infected.

Analysts say that the Stuxnet worm may have been designed to target Iran's nuclear facilities.

Iranian officials have denied the Islamic republic's first nuclear plant at Bushehr was among the addresses penetrated by the worm, but they have said that personal computers of personnel at the facility have been infected.

Iran says it needs the Bushehr plant, which had been under construction since the 1970s and was finally finished by Russia, to meet growing demand for electricity.

But the international community widely believes that Iran's atomic activities are masking a covert nuclear weapons programme, which Tehran denies.

Iran is under four sets of United Nations sanctions for its refusal to halt uranium enrichment -- the process which can be used to make nuclear fuel but also the fissile core of an atom bomb in highly purified forms.

http://news.yahoo.com/s/afp/20100929/wl_mideast_afp/irannuclearpoliticsrussiabushehr

(Return to Articles and Documents List)

New York Times
September 29, 2010

In a Computer Worm, a Possible Biblical Clue

By JOHN MARKOFF and DAVID E. SANGER

Deep inside the computer worm that some specialists suspect is aimed at slowing Iran's race for a nuclear weapon lies what could be a fleeting reference to the Book of Esther, the Old Testament tale in which the Jews pre-empt a Persian plot to destroy them.

That use of the word "Myrtus" — which can be read as an allusion to Esther — to name a file inside the code is one of several murky clues that have emerged as computer experts try to trace the origin and purpose of the rogue Stuxnet program, which seeks out a specific kind of command module for industrial equipment.

Not surprisingly, the Israelis are not saying whether Stuxnet has any connection to the secretive cyberwar unit it has built inside Israel's intelligence service. Nor is the Obama administration, which while talking about cyberdefenses has also rapidly ramped up a broad covert program, inherited from the Bush administration, to undermine Iran's nuclear program. In interviews in several countries, experts in both cyberwar and nuclear enrichment technology say the Stuxnet mystery may never be solved.

There are many competing explanations for myrtus, which could simply signify myrtle, a plant important to many cultures in the region. But some security experts see the reference as a signature allusion to Esther, a clear warning in a mounting technological and psychological battle as Israel and its allies try to breach Tehran's most heavily guarded project. Others doubt the Israelis were involved and say the word could have been inserted as deliberate misinformation, to implicate Israel.

"The Iranians are already paranoid about the fact that some of their scientists have defected and several of their secret nuclear sites have been revealed," one former intelligence official who still works on Iran issues said recently. "Whatever the origin and purpose of Stuxnet, it ramps up the psychological pressure."

So a calling card in the code could be part of a mind game, or sloppiness or whimsy from the coders.

The malicious code has appeared in many countries, notably China, India, Indonesia and Iran. But there are tantalizing hints that Iran's nuclear program was the primary target. Officials in both the United States and Israel have made no secret of the fact that undermining the computer systems that control Iran's huge enrichment plant at Natanz is a high priority. (The Iranians know it, too: They have never let international inspectors into the control room of the plant, the inspectors report, presumably to keep secret what kind of equipment they are using.)

The fact that Stuxnet appears designed to attack a certain type of Siemens industrial control computer, used widely to manage oil pipelines, electrical power grids and many kinds of nuclear plants, may be telling. Just last year officials in Dubai seized a large shipment of those controllers — known as the Simatic S-7 — after Western intelligence agencies warned that the shipment was bound for Iran and would likely be used in its nuclear program.

"What we were told by many sources," said Olli Heinonen, who retired last month as the head of inspections at the International Atomic Energy Agency in Vienna, "was that the Iranian nuclear program was acquiring this kind of equipment."

Also, starting in the summer of 2009, the Iranians began having tremendous difficulty running their centrifuges, the tall, silvery machines that spin at supersonic speed to enrich uranium — and which can explode spectacularly if they become unstable. In New York last week, Iran's president, Mahmoud Ahmadinejad, shrugged off suggestions that the country was having trouble keeping its enrichment plants going.

Yet something — perhaps the worm or some other form of sabotage, bad parts or a dearth of skilled technicians — is indeed slowing Iran's advance.

The reports on Iran show a fairly steady drop in the number of centrifuges used to enrich uranium at the main Natanz plant. After reaching a peak of 4,920 machines in May 2009, the numbers declined to 3,772 centrifuges this past August, the most recent reporting period. That is a decline of 23 percent. (At the same time, production of low-enriched uranium has remained fairly constant, indicating the Iranians have learned how to make better use of fewer working machines.)

Computer experts say the first versions of the worm appeared as early as 2009 and that the sophisticated version contained an internal time stamp from January of this year.

These events add up to a mass of suspicions, not proof. Moreover, the difficulty experts have had in figuring out the origin of Stuxnet points to both the appeal and the danger of computer attacks in a new age of cyberwar.

For intelligence agencies they are an almost irresistible weapon, free of fingerprints. Israel has poured huge resources into Unit 8200, its secretive cyberwar operation, and the United States has built its capacity inside the National Security Agency and inside the military, which just opened a Cyber Command.

But the near impossibility of figuring out where they came from makes deterrence a huge problem — and explains why many have warned against the use of cyberweapons. No country, President Obama was warned even before he took office, is more vulnerable to cyberattack than the United States.

For now, it is hard to determine if the worm has infected centrifuge controllers at Natanz. While the S-7 industrial controller is used widely in Iran, and many other countries, even Siemens says it does not know where it is being used. Alexander Machowetz, a spokesman in Germany for Siemens, said the company did no business with Iran's nuclear program. "It could be that there is equipment," he said in a telephone interview. "But we never delivered it to Natanz."

But Siemens industrial controllers are unregulated commodities that are sold and resold all over the world — the controllers intercepted in Dubai traveled through China, according to officials familiar with the seizure.

Ralph Langner, a German computer security consultant who was the first independent expert to assert that the malware had been "weaponized" and designed to attack the Iranian centrifuge array, argues that the Stuxnet worm could have been brought into the Iranian nuclear complex by Russian contractors.

"It would be an absolute no-brainer to leave an infected USB stick near one of these guys," he said, "and there would be more than a 50 percent chance of having him pick it up and infect his computer."

There are many reasons to suspect Israel's involvement in Stuxnet. Intelligence is the single largest section of its military and the unit devoted to signal, electronic and computer network intelligence, known as Unit 8200, is the largest group within intelligence.

Yossi Melman, who covers intelligence for the newspaper Haaretz and is at work on a book about Israeli intelligence over the past decade, said in a telephone interview that he suspected that Israel was involved.

He noted that Meir Dagan, head of Mossad, had his term extended last year partly because he was said to be involved in important projects. He added that in the past year Israeli estimates of when Iran will have a nuclear weapon had been extended to 2014.

"They seem to know something, that they have more time than originally thought," he said.

Then there is the allusion to myrtus — which may be telling, or may be a red herring.

Several of the teams of computer security researchers who have been dissecting the software found a text string that suggests that the attackers named their project Myrtus. The guava fruit is part of the Myrtus family, and one of the code modules is identified as Guava.

It was Mr. Langner who first noted that Myrtus is an allusion to the Hebrew word for Esther. The Book of Esther tells the story of a Persian plot against the Jews, who attacked their enemies pre-emptively.

"If you read the Bible you can make a guess," said Mr. Langner, in a telephone interview from Germany on Wednesday.

Carol Newsom, an Old Testament scholar at Emory University, confirmed the linguistic connection between the plant family and the Old Testament figure, noting that Queen Esther's original name in Hebrew was Hadassah, which is similar to the Hebrew word for myrtle. Perhaps, she said, "someone was making a learned cross-linguistic wordplay."

But other Israeli experts said they doubted Israel's involvement. Shai Blitzblau, the technical director and head of the computer warfare laboratory at Maglan, an Israeli company specializing in information security, said he was "convinced that Israel had nothing to do with Stuxnet."

"We did a complete simulation of it and we sliced the code to its deepest level," he said. "We have studied its protocols and functionality. Our two main suspects for this are high-level industrial espionage against Siemens and a kind of academic experiment."

Mr. Blitzblau noted that the worm hit India, Indonesia and Russia before it hit Iran, though the worm has been found disproportionately in Iranian computers. He also noted that the Stuxnet worm has no code that reports back the results of the infection it creates. Presumably, a good intelligence agency would like to trace its work.

Ethan Bronner contributed reporting from Israel, and William J. Broad from New York.

http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?pagewanted=all

(Return to Articles and Documents List)

Boston Globe

NKorea Vows to Strengthen Nuclear Arms

By Ali Akbar Dareini, Associated Press Writer
September 29, 2010

NEW YORK --North Korea vowed Wednesday to strengthen its nuclear weapons stockpile in order to deter a U.S. and South Korean military buildup in the region.

Speaking before the United Nations Wednesday, North Korea's Vice-Minister of Foreign Affairs Pak Kil Yon said Pyongyang is, however, ready to join nuclear nonproliferation efforts in its capacity as a nuclear weapon state.

"As long as the U.S. nuclear aircraft carriers sail around the seas of our country, our nuclear deterrent can never be abandoned but be should be strengthened further," Pak said. "This is the lesson we have drawn."

Pak defended Pyongyang's development of nuclear weapons, saying it has succeeded in preventing the Korean peninsula from being "turned into a war field scores of times."

He insisted that North Korea's stockpile of atomic weapons was exclusively for the purposes of self-defense and that his country hoped to abide by international treaties governing their use.

"As a responsible nuclear weapon state, we are willing to join in the international efforts for nuclear non-proliferation and safe management of nuclear material on an equal footing with other nuclear weapon states," he said.

North Korea's nuclear program is of intense concern because of worries the country is building its arsenal of atomic weapons. Pyongyang conducted two nuclear weapons tests in 2006 and 2009, drawing international condemnation and U.N. sanctions.

The U.S. is trying to restart stalled negotiations on North Korea's nuclear disarmament. North Korea walked out of the six-party talks last year amid international criticism of its long-range rocket launch. Prospects for resuming the talks dimmed after Pyongyang was accused of sinking of a South Korean warship in March.

Pak didn't say if his country was ready to return to talks but said a nuclear-weapon-free Korean peninsula would be achieved only if external nuclear threats are eliminated, a referrence to the U.S. presence in South Korea.

Pak denounced the U.S. as "disruptor of peace" in the Korean peninsula, saying ongoing U.S.-South Korean military exercises close to its border were provocative and causing tension.

North Korea has strongly objected to the drills, which came in response to the warship's sinking, claiming they are in preparation for an invasion.

Pak denied his country had anything to do with ship's sinking and questioned the credibility an investigation into the incident that found North Korea responsible.

http://www.boston.com/news/nation/articles/2010/09/29/nkorea_vows_to_strengthen_nuclear_arms/

(Return to Articles and Documents List)

Breitbart.com

N.Korea Leaders Must Commit Against Nukes: US

September 29, 2010
By Agence France-Presse (AFP)

The United States on Wednesday called on North Korea's leadership to make clear its support for a 2005 denuclearization pact after strongman Kim Jong-Il's youngest son took over powerful posts.

"We need to see a very clear signal that this new leadership -- or some structure in North Korea -- accepts the very clear commitments that North Korea made in 2005 to denuclearization," said Kurt Campbell, the assistant secretary of state for East Asia.

Campbell also renewed calls for North Korea to ease tensions with South Korea in the wake of March's sinking of the Cheonan vessel, which killed 46 sailors. US and South Korean investigators said the North torpedoed the ship.

"We believe in the current environment, the most important thing is for North Korea to reach out and get in the process of re-establishing a more forward-looking relationship with South Korea," said Campbell, who was addressing the National Bureau of Asian Research.

Campbell reiterated that the United States was exercising caution over developments in the secretive country, where a major party meeting anointed Kim Jong-Un to positions that make the young man heir apparent.

North Korea pledged in six-nation talks in 2005 to give up its nuclear program in return for aid and security guarantees. It bolted from the talks last year, alleging US hostility.

Pyongyang has said it is ready to return to talks but wants to be treated as a nuclear power -- a proposition firmly rejected by the United States.

North Korea's Vice Foreign Minister Pak Kil Yon, in a speech at the United Nations on Wednesday, showed no signs of compromise, pledging that Pyongyang would boost its nuclear "deterrent" against the United States.

http://www.breitbart.com/article.php?id=CNG.4daaf11c7ddd763d80932d78a88c5277.801&show_article=1

(Return to Articles and Documents List)

Times of India – India

India to get Russian Nuclear Submarine in March

By Indo-Asian News Service (IANS)
October 1, 2010

NEW DELHI: India's undersea warfare will receive a major boost after Russia transfers its nuclear-powered K-152 Nerpa attack submarine on a 10-year lease in March next year.

The governor of the Far East Khabarovsk region told reporters in Russia on Friday that the vessel is ready.

"The boat has been handed over [to the fleet] now. According to the agreement, it will be transferred to India in March next year," Vyacheslav Shport said, as quoted by the Ria Novosti.

The $900-million lease contract was drawn up after Moscow and New Delhi sealed a deal in January 2004, in which India agreed to fund part of the Nerpa's construction.

The 12,000-ton K-152 Nerpa, an Akula II class nuclear-powered attack submarine, was originally scheduled to be introduced into the Indian Navy as INS Chakra by mid-2008.

A crew of Indian submariners last year took part in sea trials of the submarine.

The boat, damaged in a fatal accident during tests last November, resumed sea trials last year in the Sea of Japan after extensive repairs.

On Nov 8, 2008, while the Nerpa was undergoing sea trials in the Sea of Japan, its on-board fire suppression system activated, releasing a deadly gas into the sleeping quarters. Three crewmembers and 17 shipyard workers were killed.

Akula II class vessels are considered the quietest and deadliest of all Russian nuclear-powered attack submarines.

http://timesofindia.indiatimes.com/india/India-to-get-Russian-nuclear-submarine-in-March/articleshow/6665645.cms

(Return to Articles and Documents List)

RIA Novosti – Russian Information Agency

Russia to Build New Radars to Deal with 'Threats'

28 September 2010

The Defense Ministry plans to put the Voronezh-DM radar station in south Russia’s Armavir into a state of operational readiness, as well as build several new radars to counter possible threats, the Space Forces commander said Tuesday.

Lt. Gen. Oleg Ostapenko also told journalists that new radar stations will be built "to replace the current radar means and maintain continuous radar control of all missile threats."

The Armavir radar will be the second facility, after the Lekhtusi complex in the Leningrad Region, to close a gap in radar coverage on Russia's western borders after the closure of radar sites in Skrunda (Latvia) in late 1998 and recently in Mukachevo and Sevastopol in Ukraine.

With an effective range of 4,000 kilometers (2,500 miles) the Voronezh class radar has capabilities similar to its predecessors, the Dnepr and Daryal, but uses less energy and is more environmentally friendly.

MOSCOW, September 28 (RIA Novosti)

http://en.rian.ru/mlitary_news/20100928/160757170.html

(Return to Articles and Documents List)

SpaceDaily.com

Russia Sends Military Satellite Into Space

By Staff Writers
Moscow, Russia (XNA)
October 01, 2010

Russia on Thursday successfully launched a military satellite, said spokesman for Russian Space Forces Alexei Zolotukhin.

A "Molniya-M" carrier rocket blasted off from the Plesetsk space center in northern Russia at 9:01 p.m. Moscow time (1701 GMT) , carrying a military satellite of "Cosmos" series, said the spokesman, adding that the launch took place in normal mode.

The launch carried out by a team from Russian Space Forces was supervised by Space Forces Commander Oleg Ostapenko.

The satellite was scheduled to enter its orbit at 9:57 p.m. Moscow time (1757 GMT), said Zolotukhin. It would enhance Russia's orbital group for military purpose, he added.

"The launches of Molniya carrier rockets from the Plesetsk space center started out in 1970 and 229 such launches have been made to-date, thus confirming the reliability of this technology," said the spokesman as quoted by the Itar-Tass news agency.

It was the last launch of a carrier rocket from the Molniya-M family, he said, adding that the Molniya-M rockets were to give way to Soyuz-2 and Angara rockets.

Source: Xinhua

http://www.spacedaily.com/reports/Russia_Sends_Military_Satellite_Into_Space_999.html

(Return to Articles and Documents List)

RIA Novosti – Russian Information Agency
What the Russian Papers Say
1 October 2010
Vzglyad

Iran Banned from Investing in Uranium Enrichment in Russia

Russian President Dmitry Medvedev has signed a decree prohibiting Iranian citizens from taking part in commercial activity related to uranium production and nuclear technology in Russia, which could cut Russian-Iranian military cooperation to zero.

The decree was signed on September 22 but made public only on Thursday, September 30. The president's press secretary said the document prohibits the delivery of battle tanks, armored vehicles, large-caliber artillery guns, combat aircraft and helicopters, warships, missiles, and the S-300 air defense missile systems to Iran.

The latter was the most painful blow for Iran, which presumably intended to use the S-300 to protect its nuclear facilities.

Medvedev's decree also stipulates bans that could be psychologically worse than the ban on the S-300 deliveries. The Russian president has prohibited Iranian authorities, citizens and legal entities from investing in Russia in any commercial operations related to uranium mining and the production and use of nuclear materials and technology.

The latter ban concerns, in particular, investment in uranium enrichment, the recycling of nuclear fuel waste, and projects related to heavy water and ballistic missile technology.

The decree has curtailed Russian-Iranian military cooperation and limited nuclear technology interaction to Russia's participation in the Bushehr nuclear power plant's construction.

Presidential aide Sergei Prikhodko emphasized that the decree will not concern the Bushehr project.

"Bushehr is fully controlled by the IAEA and there are no questions regarding the project," he said.

However, the decree effectively blocks Iran's other potential attempts to exceed the limits of this cooperation. It even prohibits Iranian officials who could be connected with Iran's nuclear weapons programs from entering or transiting Russia.

Iranian authorities have downplayed Medvedev's decree. The Iranian defense ministry said Russia's actions would not affect their defense capability and that they could do without the S-300 system because they are working on a similar project.

Analysts point out that Medvedev's decree will benefit Russia by promoting its relations with the West.

http://en.rian.ru/papers/20101001/160791192.html

(Return to Articles and Documents List)

Daily Telegraph – U.K.

Liam Fox: Defence Cuts will have 'Grave Consequences'

"Draconian" cuts to defence spending cannot be carried out while the country is at war without "grave consequences" for the Government, Dr Liam Fox has warned the Prime Minister.

By Thomas Harding, Defence Correspondent
28 September 2010

In a private letter to David Cameron seen by *The Daily Telegraph*, the Defence Secretary refuses to back any substantial reduction in the Armed Forces.

He says it risks seriously damaging troops' morale.

The letter was written the night before a National Security Council (NSC) meeting on the Strategic Defence and Security Review (SDSR). In it, Dr Fox says the Tories risk "destroying much of the reputation and capital" they have built up on defence.

The review is becoming indefensible, he suggests, warning of the "brutal reaction" from the party, press and military if "we do not recognise the dangers and continue to push for such draconian cuts at a time when we are at war".

Senior Whitehall sources suggested that his intervention was a considerable political gamble after he agreed in public that the MoD had to take the pain of cuts.

The Treasury has asked the ministry to find ten per cent savings on its annual £37billion budget and the letter will further inflame Dr Fox's relationship with George Osborne, the Chancellor. The Defence Secretary claims to have the support of other ministers.

The NSC was presented with a paper earlier this month that listed the scale of MoD cuts required to meet the Treasury's reduction in its budget.

It is understood that tens of thousands of soldiers, sailors and airmen face losing their jobs.

The Navy's plan for new aircraft carriers is under threat, and ministers have argued over replacing the Trident nuclear submarines. Its fleet of amphibious craft could be scrapped.

The RAF is likely to lose many fighters and any new Nimrod surveillance aircraft. The Territorial Army is also facing cuts.

The review has been under way for months and has been criticised by MPs and senior commanders. But this is the first time the Defence Secretary's fears have been made public.

In a document marked "for the Prime Minister's eyes only", Dr Fox writes: "Frankly, this process is looking less and less defensible as a proper SDSR and more like a "super CSR" (comprehensive spending review).

“If it continues on its current trajectory it is likely to have grave political consequences for us.”

He also warns: “Our decisions today will limit severely the options available to this and all future governments.”

Despite five months’ hard work by MoD civil servants and servicemen to examine how to make at least £4billion in savings, the cuts are “financially and intellectually virtually impossible”, he says.

Dr Fox suggests that they discuss whether “we are really prepared to see Defence spending reduced to this level”. He says: “The range of operations that we can do today we will simply not be able to do in the future.”

The Navy will have to withdraw from one of its key “standing commitments”, the Gulf, Indian Ocean or Caribbean.

Losing amphibious landing ships will leave Britain unable to mount even a relatively small operation such as the mission in Sierra Leone 10 years ago, he warns.

The nuclear deterrent will also be at severe risk of detection and oil rigs will be vulnerable to terrorist attack if the programme for the new Nimrod MR4 maritime reconnaissance plane is cancelled.

It will also affect the security of the Falklands. On the home front, the Armed Forces will struggle to provide cover for crises such as foot and mouth, firemen’s strikes, Mumbai-style attacks and the 2012 London Olympics, he warns.

The scale of cuts will “seriously damage morale across the Armed Forces” and they will coincide with a “period of major challenge (and, in all probability, significant casualties) in Afghanistan”, he says.

He concludes: “It would be a great pity if, having championed the cause of our Armed Forces and set up the innovation of the NSC, we simply produced a cuts package. Cuts there will have to be. Coherence, we cannot do without, if there is to be any chance of a credible narrative.”

In a sign of ministers’ concerns, the NSC yesterday reviewed Dr Fox’s work and asked for more research into the impact of possible cuts. The council asked for more “efficiency savings” in equipment procurement and further analysis of possible cuts in programmes including the two new aircraft carriers. Mr Cameron told the NSC that the defence review would not be allowed to undermine operations in Afghanistan.

Downing Street confirmed that Mr Cameron was aware of Dr Fox’s “concerns”. A spokesman said: “You would expect the Secretary of State to make robust representations.”

http://www.telegraph.co.uk/news/newstopics/politics/defence/8031383/Liam-Fox-defence-cuts-will-have-grave-consequences.html

(Return to Articles and Documents List)

The Independent – U.K.

Britain and France may Share Nuclear Deterrent

Joint submarine patrols were rejected by Brown before the election, but they are now seen as an answer to defence cuts

By John Lichfield in Paris and Kim Sengupta
Thursday, 30 September 2010

The possibility of a "shared" UK-French nuclear deterrent is set to be on the agenda of a summit between David Cameron and Nicolas Sarkozy in London this autumn.

A politically explosive proposal for joint Franco-British nuclear-submarine patrols – an idea sunk without trace in the recent past – has been brought back to the surface by the draconian defence cuts in both countries.

Although talks are still at a preliminary stage, officials in Paris say that the idea is one possibility for cost-saving military co-operation which is likely to be discussed by the Prime Minister and the President at the annual Franco-British summit in London in early November.

A senior British defence official acknowledged last night that the possibility of sharing nuclear deterrence capability with the French remains on the table, adding that a "number of options are being studied".

The official, who has advised the Government on nuclear policy, pointed out that although the Defence Secretary, Liam Fox, has vowed the UK will keep its independent nuclear deterrent, the £20bn cost of replacing Trident meant that "one had to adjust one's sights".

The insistence of Chancellor George Osborne that the money would have to come from the defence budget rather than the Treasury has made looking at cheaper options even more imperative.

The idea of joint submarine patrols has been discussed before – most recently in March – when it was floated by President Sarkozy but rejected by Gordon Brown. The change of government in the UK, and the sheer scale of the threatened defence cuts, have revived the discussions but French and British officials warn that technical and political obstacles have not yet been overcome.

The proposition is simple – if politically fraught. France and Britain each have four nuclear-armed submarines. Each has at least one submarine permanently on patrol, ready to respond to a nuclear attack on its home country. If the two countries pooled their fleets, there could be occasions when only one submarine – either British or French – would be stationed at the bottom of the ocean ready to retaliate against an attack on either country.

This would reduce the number of submarines that each country has to maintain in order to preserve a "credible" nuclear deterrent. It would also help to solve a huge political problem for the Coalition Government by reducing the cost of replacing the existing Trident submarines sometime after 2015.

Sharing with the French is still "just a discussion point" but could help to address that problem, the defence official said.

The idea is believed to have been discussed by Mr Brown and Mr Sarkozy in March this year and ultimately sunk by Mr Brown as politically unfeasible in an election year. Similar discussions on Anglo-French nuclear co-operation are believed to have occurred in the past, going back to the Edward Heath government in the early 1970s.

Officials in Paris say that new impetus has been given to the idea by the huge budget deficits, and swingeing defence spending cuts, faced by both nations. Other ideas for military "pooling" said to be under discussion before the Franco-British summit include a revised version of a recently rejected proposal for a "shared" use of aircraft carriers and a joint programme for building a new generation of frigates.

Discussions in the past have been hampered by mutual suspicion and fear of negative domestic political and media reactions. The French did not like America's control over the supposedly independent UK nuclear deterrent. Britain suspected France of wanting to create a European defence policy to undermine Nato. These doubts have now been eased, on both sides of the Channel (and the Atlantic), by President Sarkozy's decision to return France to the joint military command of the Atlantic alliance. Politically, however, it is accepted that the idea might still be difficult to swallow in both countries.

Could France be relied upon to retaliate against an attack on the UK, if that might then mean nuclear retaliation against France? And vice versa.

Officials draw attention, however, to an interesting but little-reported comment by President Sarkozy in a speech in Cherbourg in March 2008, just after talks with Mr Brown. "Together with the United Kingdom," he said, "we have taken a major decision: it is our assessment that there can be no situation in which the vital interests of either of our two nations could be threatened without the vital interests of the other also being threatened."

The possibility of Franco-British nuclear co-operation has been a buzz subject for several weeks in defence think-tanks in both countries. Experts accept that (even though it is more than 200 years since France and Britain fought each other) the old suspicions and rivalries remain.

But they also point out that, in practical terms, a nuclear attack on Britain by a foreign aggressor would also be an attack on France (and vice versa). If British cities were devastated by a nuclear attack, most of northern France would be rendered uninhabitable.

Like Britain's four-string Trident submarine fleet based in western Scotland, France's nuclear deterrent or Force de Frappe consists of four submarines, each armed with 16 missiles. The fleet, currently reduced to three with a new submarine under construction, is based at L'Ile Longue, opposite the port of Brest in Brittany.

* Labour is set to fight the next general election on a pledge to halt the proposed £20bn Trident upgrade. Ed Miliband said yesterday that he wanted Britain to retain an independent nuclear deterrent but questioned the need for the like-for-like replacement supported by the Conservative Party.

http://www.independent.co.uk/news/world/politics/britain-and-france-may-share-nuclear-deterrent-2093539.html

(Return to Articles and Documents List)

Knoxville News Sentinel Blog
September 28, 2010

Taking a Close Look at W84 Warhead

By Frank Munger

The National Nuclear Security Administration today announced that Pantex had completed the disassembly and inspection of the first W84 warhead since 1998, a process that's needed to confirm whether or not the system has experienced any safety-related concerns due to aging.

The W84 warhead entered the U.S. nuclear stockpile in 1983 and remains in the inactive stockpile.

The NNSA said the Pantex milestone marks the "beginning of the disassembly and inspection process for the W84."

"The project team consisting of members from NNSA, Lawrence Livermore National Laboratory, Sandia National Laboratories in California and Pantex worked together for 24 months and completed the project ahead of schedule," the federal agency said.

In a statement, NNSA Deputy Administrator Don Cook said, "Disassembly and inspection of this system allows us to look at its components to find out how the weapon has aged. This analysis helps us maintain a safe, secure and effective stockpile without the need for nuclear testing. The scientific and technical knowledge we gain when we disassemble a weapon is invaluable as we look across all of our systems."

Completion of "W84 Seamless Safety for the 21st Century" project (SS-21) was part of the NNSA's top ten priorities for Fiscal Year 2010.

The NNSA said Lawrence Livermore and Sandia designed the W84 warhead, which supported part of the nation's nuclear cruise missiles programs.

According to today's release, "The U.S. produced the W84 warhead in the 1980s, and the warhead remains in the inactive stockpile. The delivery platform was the BGM-109G Gryphon Ground Launched Cruise Missile which was decommissioned as part of the signing of the Intermediate-Range Nuclear Forces Treaty. The Initial Operations Capability date for the W84 was December 1983."

There was no immediate response from Y-12 regarding the Oak Ridge schedule or plans for dismantling and analyzing W84 parts, but the plant's 10-year site plan indicates that the W84 is on the list of 19 weapon systems for which the plant must prepare capabilities to dismantle and disposition parts.

That list includes the B43, B53, B61 and B83 bombs, and these warheads: W48, W49, W59 (Minuteman I), W62 (Minuteman III), W68 (Poseidon), W69 (Short-Range Attack Missile), W70 (Lance), W71 (Spartan), W76 (Trident I), W78 (Minuteman III), W79, W80, W84, W87 (Peacekeeper) and W88 (Trident II).

http://blogs.knoxnews.com/munger/2010/09/taking_a_look_at_w84_warheads.html

(Return to Articles and Documents List)

San Francisco Business Times
Wednesday, September 29, 2010

Livermore Lab Works with WeatherBug on Emergency System

San Francisco Business Times - by Steven E.F. Brown

Lawrence Livermore National Laboratory will work with AWS Convergence Technologies, which owns the "WeatherBug" system, on a weather information system to be used during emergencies like a terrorist attack.

The WeatherBug Network is made up of some 8,000 observation stations around the country.

If there's a chemical, biological or nuclear attack, the system will be used to give information on how radiation or dangerous chemicals might be spreading in the atmosphere.

Anyone who's seen sunsets in San Francisco turn spectacular after a distant Sierra Nevada forest fire knows that particulates in the air can travel tremendous distances.

AWS, based in Germantown, Md., signed a memorandum of understanding, or MOU, with the Department of Energy and the National Nuclear Security Administration for this project, which is a public-private partnership.

Weather data will be used at the National Atmospheric Release Advisory Center, which studies and tracks "plumes" of material released into the air.

Lawrence Livermore National Laboratory started in 1952 as a Cold War atomic weapons center, but has since expanded into many areas of research, including weather and climate studies, which require vast computing power to be accurate.

The lab is run for the DOE by the University of California and a number of private businesses, including both Bechtel Corp. and URS Corp. (NYSE: URS) in San Francisco.

http://sanfrancisco.bizjournals.com/sanfrancisco/stories/2010/09/27/daily37.html

(Return to Articles and Documents List)

Global Security Newswire

U.S. May Disable Some Submarine-Based Nuclear Arms Capacity

Thursday, September 30, 2010
By Elaine M. Grossman

WASHINGTON -- To implement the U.S.-Russian "New START" arms control agreement, Washington is likely to "inactivate" one-sixth of its capacity to launch nuclear weapons from submarines, according to defense officials (see *GSN*, Sept. 27).

The alteration, if performed, would involve rendering unusable four ballistic missile launch tubes on each of 14 Trident submarines. Today the vessels feature 24 active launch tubes, each containing a single D-5 ballistic missile. The change would bring that number down to 20 missiles per boat.

"Nothing has been decided because the final force structure [under the treaty] has not been chosen," said one Defense Department official, who was not authorized to speak publicly about the issue and requested anonymity in this article. "But it is about a 98 percent certainty that that's what we'll do."

Though technical details remain uncertain regarding how the modifications would be made, U.S. officials anticipate the changes would be verifiable by Russian arms control inspectors.

The partial inactivation of launch tubes would also almost certainly be reversible, allowing Washington to meet treaty caps but retain some flexibility in how its smaller nuclear arsenal is arrayed in the future, defense sources said.

U.S. President Barack Obama and Russian President Dmitry Medvedev signed the New START agreement in April. Now pending before U.S. and Russian lawmakers for ratification, it limits each side to 1,550 deployed warheads aboard 700 strategic delivery vehicles, such as aircraft, submarine-launched ballistic missiles and ground-based ICBMs. Another 100 delivery platforms could be kept in reserve.

Once the treaty enters into force, the Obama administration plans to "deploy no more than 240 Trident 2 SLBMs at any one time," James Miller, the principal deputy defense undersecretary for policy, told a Senate committee in July.

Just 12 of today's 14 Trident submarines are operational, with two boats in overhaul at any given time. Warheads or missiles in vessels undergoing the periodic maintenance are not counted under New START limits.

The Defense Department currently fields 288 Trident D-5 missiles, filling each of the 24 launch tubes aboard 12 deployed submarines. As New START is implemented and the launch-tube modifications are made, the Navy would be able to reduce to the Pentagon objective of 240 missiles using this math: 20 missiles multiplied by 12 operational vessels.

The Pentagon's Nuclear Posture Review -- a major assessment of strategy and forces released in April -- stated that the Navy will continue to field 14 total ballistic-missile submarines for the time being, but might reduce to 12 such boats before the end of the decade. With two of those typically in overhaul, just 10 would be regarded as operational day to day.

If the Defense Department goes forward with trimming its Trident submarine fleet in the coming years, it would have the option of reversing the launch-tube inactivation and renewing its capacity for the remaining 10 operational vessels to carry 24 missiles apiece, maintaining the level of 240 missiles fielded across the fleet, officials said.

The launch-tube measure could thus be seen as a "bridge" to the probable reduction in the quantity of ballistic-missile submarines by the end of the decade, said Hans Kristensen, director of the Nuclear Information Project at the Federation of American Scientists. "Otherwise, they'd have to wait till the end of the decade to reduce missiles out there," he said in an interview this week.

However, some observers believe it might be politically difficult for the Navy to return to loading 24 nuclear missiles per vessel later in the decade. After having maintained nuclear deterrence for several years by sailing with just 20 weapons on each submarine, it could appear that an additional four would be unnecessary, the argument goes.

"If they go to sea with only 20, that would cause people to re-evaluate the requirements for the D-5 life-extension program, which assumes 24 missiles," said one industry analyst, referring to the Navy's current effort to field 108 updated versions of the submarine-based weapon. "So if you drop four missiles per boat, then you could reduce the buy by 48 missiles."

The Navy plans to introduce the life-extension version of the D-5 missile into the fleet in three years. The modified arms will include newly produced rocket motors, remanufactured flight hardware and modern guidance instruments.

A decision to reduce the number of missiles on Trident vessels "would also say that the option of 24 tubes per boat on the new submarine design doesn't look like it would be valid anymore," said the analyst, who asked not to be named in discussing sensitive fielding options.

The Navy's next-generation ballistic missile submarine, called the SSBN(X), could have as few as 16 launch tubes or as many as 24, with design details expected to go before a top-level Pentagon review board for decision in November, defense sources said.

The Nuclear Posture Review asserted that a reduction to 10 operational submarines "will not affect the number of deployed nuclear warheads" on the vessels. The Ohio-class submarines currently carry a total 1,152 warheads and, once the New START reductions are taken, they would likely carry just under 1,100, Kristensen estimated.

If the Pentagon declines to reactivate the four launch tubes once the submarine fleet shrinks to 10 deployed boats, the Navy could retain the same number of warheads across its remaining 200 missiles by arming them with five to six warheads apiece, instead of today's average of four, Kristensen said.

Taking policy considerations into account, a reversible inactivation of the launch tubes also offers Obama administration leaders a "hedge" against any resurgence in Russian strategic forces or some other strategic surprise, officials said. The New START agreement includes a clause that allows either side to withdraw if it determines that "extraordinary events" have jeopardized its national security.

The nation has seven years to take reductions in its force structure, following the accord's entry into force.

Defense Department engineers are just now beginning to assess how they might suspend the usability of four launch tubes on each boat, according to Pentagon sources.

Under one engineering approach, the Navy might simply remove the gas pressure system that allows a ballistic missile to be ejected by "cold launch," before its rocket motors kick in. Another method could involve inserting a narrow sleeve into each tube that would make it impossible for a D-5 missile to fit inside.

A third option might be to replace each of the four D-5s with a "ballast can," a 15-foot weight that a submarine could carry for stability when a missile is not in its tube, according to sources.

"That's what the Navy has to figure out," the Pentagon official said.

Beyond the submarine leg of the U.S. nuclear triad, Washington under New START expects to "retain up to 420 of the current 450 Minuteman 3 ICBMs, each with a single warhead," Miller told the Senate Armed Services Committee on July 20. "And we plan to retain up to 60 nuclear-capable B-2A and B-52H heavy bombers, while converting remaining nuclear-capable B-1B bombers and some B-52 bombers as well to a conventional-only capability."

http://www.globalsecuritynewswire.org/gsn/nw_20100930_1061.php

(Return to Articles and Documents List)

London Guardian – U.K.

Stuxnet Worm Heralds New Era of Global Cyberwar

Attack aimed at Iran nuclear plant and recently revealed 2008 incident at US base show spread of cyber weapons
By Peter Beaumont
Thursday, 30 September 2010

The memory sticks were scattered in a washroom of a US military base in the Middle East that was providing support for the Iraq war.

They were deliberately infected with a computer worm – the undisclosed foreign intelligence agency behind the operation was counting on the fallibility of human nature.

According to those familiar with the events, it calculated a soldier would pick up one of the memory sticks, pocket it and – against regulations – eventually plug it into a military laptop.

They were correct.

The result was the delivery of a self-propagating malicious worm into the secure computer system of the US military's central command – Centcom – which would take 14 months to finally eradicate in an operation codenamed Buckshot Yankee.

That attack took place in 2008 and was only acknowledged by the Pentagon this August. It is strikingly similar to the recently disclosed cyber attack on Iran's nuclear facilities with the Stuxnet worm, which also appears to have used contaminated hardware in an attempt to cripple Iran's nuclear programme, rather than using bombs dropped from the air.

Where these two incidents differ from previous high profile cyber attacks, including some backed by states, is the fact that they have gone far beyond cyber annoyance – even on a grand scale – and pushed towards real cyberwar.

Like the attack on Centcom's computers, the Stuxnet worm, which Iran admits has affected 30,000 of its computers, was a sophisticated attack almost certainly orchestrated by a state, a sabotage operation using computer code as a weapon. It appears intelligence operatives were used to deliver the worm to its goal.

Its primary target, computer security experts say, was an off-the-shelf Siemens-manufactured control system used widely by Iran – not least in its nuclear facilities.

Yesterday Iran confirmed that the worm had been found on laptops at the Bushehr nuclear reactor – which had been due to go online next month but has now been delayed. It denied the Stuxnet worm had infected the main operating system or been responsible for the problems.

"I say firmly that enemies have failed so far to damage our nuclear systems through computer worms despite all of their measures and we have cleaned our systems," Ali Akbar Salehi, the head of Iran's atomic energy agency, told the Iranian Students News Agency this week.

If the Stuxnet attack on Iran has suggested what a limited act of cyber sabotage might look like, on Tuesday the United States attempted to imagine what an all-out cyberwar might look like and whether it was equipped to deal with it.

In an exercise named Cyber Storm III involving government agencies and 60 private sector organisations including the US banking, chemical, nuclear energy and IT sectors, it presented a scenario where America was hit by a coordinated cyber shock and awe campaign, hitting 1,500 different targets. The results of the exercise have not been released.

One of those who believes that cyberwar has finally come of age is James Lewis of the Centre for Strategic and International Studies in Washington. Lewis says that while previous large scale hacking attacks including a Russian attack on Estonia were largely significant for their annoyance value, Stuxnet and the attack on CentCom represented the real use of malicious programmes as significant weapons.

"Cyberwar is already here," says Lewis. "We are in the same place as we were after the invention of the airplane. It was inevitable someone would work out how to use planes to drop bombs.

"Militaries will now have a cyberwar capability in their arsenals. There are five already that have that capacity including Russia and China."

Of those Lewis says he believes only three have both the motivation and organisational and technical capacity to mount the Stuxnet attack on Iran: the US, Israel and the UK.

Lewis says too that while the destructive potential of cyberwar was once seen as somewhat notional, that perception changed in the US in particular after a deliberately staged remote hack of an electric generator at the Idaho National Laboratory. The attack, which came via the internet, demonstrated that infrastructure – like power plants – could be persuaded to destroy itself.

"There is growing concern that there has already been hostile reconnaissance of the US electricity grid," he said.

Last year the Wall Street Journal quoted US intelligence officials describing how cyber spies had charted the on-off controls for large sections of the US grid and its vulnerability to hacking.

The head of the Pentagon's newly inaugurated US Cyber Command at Fort Meade, General Keith Alexander, has said in recent remarks that it is not a question of if but when America is attacked by something like the Stuxnet worm.

In recent testimony to Congress, Alexander underlined how the cyberwar threat has rapidly evolved in the last three years, describing two of the most high-profile attacks on nations – the 2007 assault on Estonian and the 2008 attack on Georgia during its war with Russia – which were both blamed on Mosow.

Those were both so-called "denial of service" attacks that briefly disabled computer networks. It is not that kind of cyberwar that is frightening America's top cyber warrior. "What concerns me the most," he told the House armed services committee, "are destructive attacks." Like Stuxnet.

Alexander is one of those who favours binding agreements – similar to nuclear weapons treaties – with countries like Russia limiting the retention and use of cyberwar technology.

One the problems that will confront states in this new era, it has become increasingly clear, is identifying precisely who is behind any given attack.

Some analysts believe Israel is the most likely culprit in the Stuxnet attack on Iran – perhaps through its cyberwar Unit 8200, which has been increasingly heavily resourced.

They point to a reference in the worm's code to Myrtus – an oblique refererence to the biblical Esther and Jewish pre-emption of a plot to kill them. Other analysts argue that writers of malicious computer code are now so sophisticated that they deliberately plant red herrings to put investigators off the scent.

Dave Clemente, a researcher into conflict and technology at the Royal United Services Institute at Chatham House, argues that where once the threat from cyberwar was "hyped ... reality has quickly caught up".

"You look at the Stuxnet worm. It is of such complexity it could only be a state behind it."

Clemente points to the fact that the attack used four separate unpublicised flaws in the operating system of the Iranian nuclear plant at Bushehr to infect it. Other experts note that Stuxnet used genuine verification code stolen from a Taiwanese company and that the worm's designers had built in safeguards to limit the amount of collateral damage it would cause.

"The US and the UK are now putting large amounts of resources into cyber warfare, in particular defence against it," adds Clemente. "We have a cyber command now operating in the US and in the UK there is now a cyber security operations centre in GCHQ and a new office of cyber sWoecurity in the Cabinet Office.

"What I think you can say about Stuxnet is that cyberwar is now very real. This appears to be the first instance of a destructive use of a cyberwar weapon."

http://www.guardian.co.uk/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar

(Return to Articles and Documents List)

The Economist – Britain

The Meaning of Stuxnet

A sophisticated "cyber-missile" highlights the potential—and limitations—of cyberwar
September 30th 2010

IT HAS been described as "amazing", "groundbreaking" and "impressive" by computer-security specialists. The Stuxnet worm, a piece of software that infects industrial-control systems, is remarkable in many ways. Its unusual complexity suggests that it is the work of a team of well-funded experts, probably with the backing of a national government, rather than rogue hackers or cyber-criminals. It is designed to infect a particular configuration of a particular type of industrial-control system—in other words, to disrupt the operation of a specific process or plant. The Stuxnet outbreak has been concentrated in Iran, which suggests that a nuclear facility in that country was the intended target.

This is, in short, a new kind of cyber-attack. Unlike the efforts to disrupt internet access in Estonia or Georgia (blamed on Russia), or the attacks to break into American systems to steal secrets (blamed on China), this was a weapon aimed at a specific target—it has been called a "cyber-missile". One or more governments (the prime suspects are Israel and America) were probably behind it. After years of speculation about the potential for this sort of attack, Stuxnet is a worked example of cyberwar's potential—and its limitations.

Much of the discussion of cyberwar has focused on the potential for a "digital Pearl Harbour", in which a country's power grids and other critical infrastructure are disabled by attackers. Many such systems are isolated from the internet for security reasons. Stuxnet, which exploits flaws in Microsoft Windows to spread on to stand-alone systems via USB memory sticks, shows they are more vulnerable than most people thought. The outbreak emphasises the importance of securing industrial-control systems properly, with both software (open-source code can be more easily checked for security holes) and appropriate policies (banning the use of memory sticks). "Smart" electricity grids, which couple critical infrastructure to the internet, must be secured carefully.

Stuxnet is also illuminating in another way: it reveals the potential for cyber-weapons that target specific systems, rather than simply trying to cause as much mayhem as possible. It infected several plants in Germany, for example, but did no harm because they were not the target it was looking for. Such specificity, along with the deniability and difficulty of tracing a cyber-weapon, has obvious appeal to governments that would like to disable a particular target while avoiding a direct military attack—and firms interested in sabotaging their rivals.

Cyberwar is not declared

But the worm also highlights the limitations of cyber-attacks. Iran admits that some computers at its Bushehr nuclear plant were infected, but says no damage was done. The target may have been the centrifuges at its nuclear refinery at Natanz. Last year the number of working centrifuges at Natanz dropped, though it is unclear whether this was the result of Stuxnet. Even if it was, the attack will only have delayed Iran's nuclear programme: it will not have shut it down altogether. Whoever is behind Stuxnet may feel that a delay is better than nothing. But a cyber-attack is no substitute for a physical attack. The former would take weeks to recover from; the latter, years.

Stuxnet may have failed to do the damage its designers intended, but it has succeeded in undermining the widespread assumption that the West would be the victim rather than the progenitor of a cyber-attack. It has also illustrated the murkiness of this sort of warfare. It is rarely clear who is attacking whom. It is hard to tell whether a strike has been successful, or indeed has happened at all. This, it seems, is what cyberwar looks like. Get used to it.

http://www.economist.com/node/17147862?story_id=17147862&fsrc=rss

(Return to Articles and Documents List)

Wall Street Journal
OPINION
Review & Outlook
September 29, 2010

A Modern Major-General

Boy military genius in Pyongyang.
Page – A20

It's a fair bet that Kim Jong Eun probably can't quote the fights historical in order categorical. But considering his rumored education at a Swiss boarding school, he might understand equations, both simple and quadratical. Which suffices, we suppose, to make the 26-year-old son of Kim Jong Il the very model of a modern Major-General.

Modern, that is, in a North Korean kind of way. On Tuesday, the younger Kim was elevated to four-star rank at a Communist Party meeting, the first such conclave in 30 years. Also elevated were his aunt and a family friend, both of them no doubt formidable military minds. Pyongyang watchers say this means Jong Eun is now likely to replace his ailing father, though there may be some kind of regency period. But who knows? It's not as if the Kim family held a press conference.

What we can say is that the episode is another reminder of the folly of engaging Pyongyang, the prospect of which is again being discussed after the elder Kim put out feelers that he would like to return to the six party talks. We are supposed to believe we can trust the nuclear-disarmament promises of a dynastic dictatorship that elevates a boy-man to help run the country's military. Next we'll hear that the kid is secretly a "reformer," a fact the U.S. can exploit if only we send a check for a few billion dollars to the new general.

Then again, it isn't often that North Korea finds itself in a state of political flux and disarray. The Obama Administration could inspire more change if, instead of trying to find fresh ways of sustaining the Kim regime, it brought down all the pressure it could bear to crack it. Refusing to return to the talks would be one step in that direction; increasing support for antiregime radio stations based in South Korea would be another.

In the younger Kim, the U.S. faces a general who knows less of military tactics—or the world—than a novice in a nunnery. Seeking his downfall is what Gilbert and Sullivan would call a smattering of elemental strategy.

http://online.wsj.com/article/SB10001424052748703882404575520022141358174.html

(Return to Articles and Documents List)

Jerusalem Post – Israel
OPINION

Column one: The Lessons of Stuxnet

A war ends when one side permanently breaks its enemy's ability and will to fight it. This has clearly not happened in Iran.
By CAROLINE B. GLICK
October 1, 2010

There's a new cyber-weapon on the block. And it's a doozy. Stuxnet, a malicious software, or malware, program was apparently first discovered in June.

Although it has appeared in India, Pakistan and Indonesia, Iran's industrial complexes – including its nuclear installations – are its main victims.

Stuxnet operates as a computer worm. It is inserted into a computer system through a USB port rather than over the Internet, and is therefore capable of infiltrating networks that are not connected to the Internet.

Hamid Alipour, deputy head of Iran's Information Technology Company, told reporters Monday that the malware operated undetected in the country's computer systems for about a year.

After it enters a network, this super-intelligent program figures out what it has penetrated and then decides whether or not to attack. The sorts of computer systems it enters are those that control critical infrastructures like power plants, refineries and other industrial targets.

Ralph Langner, a German computer security researcher who was among the first people to study Stuxnet, told various media outlets that after Stuxnet recognizes its specific target, it does something no other malware program has ever done. It takes control of the facility's SCADA (supervisory control and data acquisition system) and through it, is able to destroy the facility.

No other malware program has ever managed to move from cyberspace to the real world. And this is what makes Stuxnet so revolutionary. It is not a tool of industrial espionage. It is a weapon of war.

From what researchers have exposed so far, Stuxnet was designed to control computer systems produced by the German engineering giant Siemens. Over the past generation, Siemens engineering tools, including its industrial software, have been the backbone of Iran's industrial and military infrastructure. Siemens computer software products are widely used in Iranian electricity plants, communication systems and military bases, and in the country's Russian-built nuclear power plant at Bushehr.

The Iranian government has acknowledged a breach of the computer system at Bushehr. The plant was set to begin operating next month, but Iranian officials announced the opening would be pushed back several months due to the damage wrought by Stuxnet. On Monday, Channel 2 reported that Iran's Natanz uranium enrichment facility was also infected by Stuxnet.

On Tuesday, Alipour acknowledged that Stuxnet's discovery has not mitigated its destructive power.

As he put it, "We had anticipated that we could root out the virus within one to two months. But the virus is not stable and since we started the cleanup process, three new versions of it have been spreading."

While so far no one has either taken responsibility for Stuxnet or been exposed as its developer, experts who have studied the program agree that its sophistication is so vast that it is highly unlikely a group of privately financed hackers developed it. Only a nation-state would have the financial, manpower and other resources necessary to develop and deploy Stuxnet, the experts argue.

Iran has pointed an accusatory finger at the US, Israel and India. So far, most analysts are pointing their fingers at Israel. Israeli officials, like their US counterparts, are remaining silent on the subject.

While news of a debilitating attack on Iran's nuclear installations is a cause for celebration, at this point, we simply do not know enough about what has happened and what is continuing to happen at Iran's nuclear installations to make any reasoned evaluation about Stuxnet's success or failure. Indeed, *The New York Times* has argued that since Stuxnet worms were found in Siemens software in India, Pakistan and Indonesia as well as Iran, reporting, "The most striking aspect of the fast-spreading malicious computer program... may not have been how sophisticated it was, but rather how sloppy its creators were in letting a specifically aimed attack scatter randomly around the globe."

ALL THAT we know for certain is that Stuxnet is a weapon and it is currently being used to wage a battle. We don't know if Israel is involved in the battle or not. And if Israel is a side in the battle, we don't know if we're winning or not.

But still, even in our ignorance about the details of this battle, we still know enough to draw a number of lessons from what is happening.

Stuxnet's first lesson is that it is essential to be a leader rather than a follower in technology development. The first to deploy new technologies on a battlefield has an enormous advantage over his rivals. Indeed, that advantage may be enough to win a war.

But from the first lesson, a second immediately follows. A monopoly in a new weapon system is always fleeting. The US nuclear monopoly at the end of World War II allowed it to defeat Imperial Japan and bring the war to an end in allied victory.

Once the US exposed its nuclear arsenal, however, the Soviet Union's race to acquire nuclear weapons of its own began. Just four years after the US used its nuclear weapons, it found itself in a nuclear arms race with the Soviets. America's possession of nuclear weapons did not shield it from the threat of their destructive power.

The risks of proliferation are the flipside to the advantage of deploying new technology. Warning of the new risks presented by Stuxnet, Melissa Hathaway, a former US national cybersecurity coordinator, told the Times, "Proliferation is a real problem, and no country is prepared to deal with it. All of these [computer security] guys are scared to death. We have about 90 days to fix this [new vulnerability] before some hacker begins using it."

Then there is the asymmetry of vulnerability to cyberweapons. A cyberweapon like Stuxnet threatens nation-states much more than it threatens a non-state actor that could deploy it in the future. For instance, a cyber-attack of the level of Stuxnet against the likes of Hizbullah or al-Qaida by a state like Israel or the US would cause these groups far less damage than a Hizbullah or al-Qaida cyber-attack of the quality of Stuxnet launched against a developed country like Israel or the US.

In short, like every other major new weapons system introduced since the slingshot, Stuxnet creates new strengths as well as new vulnerabilities for the states that may wield it.

As to the battle raging today in Iran's nuclear facilities, even if the most optimistic scenario is true, and Stuxnet has crippled Iran's nuclear installations, we must recognize that while a critical battle was won, the war is far from over.

A war ends when one side permanently breaks its enemy's ability and will to fight it. This has clearly not happened in Iran.

Iranian President Mahmoud Ahmadinejad made it manifestly clear during his visit to the US last week that he is intensifying, not moderating, his offensive stance towards the US, Israel and the rest of the free world. Indeed, as IDF Deputy Chief of Staff Maj.-Gen. Benny Ganz noted last week, "Iran is involved up to its neck in every terrorist activity in the Middle East."

So even in the rosiest scenario, Israel or some other government has just neutralized one threat – albeit an enormous threat – among a panoply of threats that Iran poses. And we can be absolutely certain that Iran will take whatever steps are necessary to develop new ways to threaten Israel and its other foes as quickly as possible.

What this tells us is that if Stuxnet is an Israeli weapon, while a great achievement, it is not a revolutionary weapon. While the tendency to believe that we have found a silver bullet is great, the fact is that fielding a weapon like Stuxnet does not fundamentally change Israel's strategic position. And consequently, it should have no impact on Israel's strategic doctrine.

In all likelihood, assuming that Stuxnet has significantly debilitated Iran's nuclear installations, this achievement will be a one-off. Just as the Arabs learned the lessons of their defeat in 1967 and implemented those lessons to great effect in the war in 1973, so the Iranians – and the rest of Israel's enemies – will learn the lessons of Stuxnet.

SO IF we assume that Stuxnet is an Israeli weapon, what does it show us about Israel's position vis-à-vis its enemies? What Stuxnet shows is that Israel has managed to maintain its technological advantage over its enemies. And this is a great relief. Israel has survived since 1948 despite our enemies' unmitigated desire to destroy us because we have continuously adapted our tactical advantages to stay one step ahead of them. It is this adaptive capability that has allowed Israel to win a series of one-off battles that have allowed it to survive.

But again, none of these one-off battles were strategic game-changers. None of them have fundamentally changed the strategic realities of the region. This is the case because they have neither impacted our enemies' strategic aspiration to destroy us, nor have they mitigated Israel's strategic vulnerabilities. It is the unchanging nature of these vulnerabilities since the dawn of modern Zionism that gives hope to our foes that they may one day win and should therefore keep fighting.

Israel has two basic strategic vulnerabilities.

The first is Israel's geographic minuteness, which attracts invaders. The second vulnerability is Israel's political weakness both at home and abroad, which make it impossible to fight long wars.

Attentive to these vulnerabilities, David Ben- Gurion asserted that Israel's military doctrine is the twofold goal to fight wars on our enemies' territory and to end them as swiftly and as decisively as possible. This doctrine remains the only realistic option today, even if Stuxnet is in our arsenal.

It is important to point this plain truth out today as the excitement builds about Stuxnet, because Israel's leaders have a history of mistaking tactical innovation and advantage with strategic transformation. It was our leaders' failure to properly recognize what happened in 1967 for the momentary tactical advantage it was that led us to near disaster in 1973.

Since 1993, our leaders have consistently mistaken their adoption of the West's land-forpeace paradigm as a strategic response to Israel's political vulnerability. The fact that the international assault on Israel's right to exist has only escalated since Israel embraced the landfor- peace paradigm is proof that our leaders were wrong. Adopting the political narrative of our enemies did not increase Israel's political fortunes in Europe, the US or the UN.

So, too, our leaders have mistaken Israel's air superiority for a strategic answer to its geographical vulnerability. The missile campaigns the Palestinians and Lebanese have waged against the home front in the aftermath of Israel's withdrawals from Gaza and south Lebanon show clearly that air supremacy does not make up for geographic vulnerability. It certainly does not support a view that strategic depth is less important than it once was.

We may never know if Stuxnet was successful or if Stuxnet is Israeli. But what we do know is that we cannot afford to learn the wrong lessons from its achievements.

http://www.jpost.com/Opinion/Columnists/Article.aspx?id=189823

(Return to Articles and Documents List)