

From: [REDACTED]
Sent: 2013-10-15T06:09:46-06:00
Subject: Today's USSTRATCOM News Brief - 15 October 2013
Received: 2013-10-15T06:10:07-06:00
[15 October 2013 USSTRATCOM News Briefs.docx](#)
[smime.p7s](#)

P3/b(3)

10 USC 130b

Good Morning Ladies and Gentlemen,

There will be no DoD Early Bird today. The Early Bird team is on furlough due to the lapse in government funding.

US Strategic Command Today's News Briefs 15 Oct 2013

The USSTRATCOM News Briefs are a daily compilation of published current news, transcripts, and commentary related to USSTRATCOM missions, prepared by the USSTRATCOM public affairs office. Reproduction or redistribution for private use or gain is subject to original copyright restrictions.

If you would like to be added to or removed from this distribution list, send your request to [Stratcom News Briefs](#) or call the STRATCOM Public Affairs Office at 402-294-4130.

ARTICLES OF INTEREST:

Cyberspace

[Report: NSA collecting email and IM contacts globally](#)

USA Today, Melanie Eversley & Byron Acohido

The NSA is collecting email and instant messaging contacts from overseas points, reports indicate. The National Security Agency has been collecting contacts from people's personal email address books and instant messaging accounts in an effort to d...

[Defense networks vulnerable to cyberattack: Expert](#)

CNBC, Jennifer Schlesinger

The U.S. government shutdown that began Oct. 1 leaves cybersecurity experts fearing the Department of Defense's computer networks may be more at risk. While Democrats and Republicans continue to battle it out, foreign adversaries may be taking advan...

[N.S.A. Director Firmly Defends Surveillance Efforts](#)

New York Times, David E. Sanger and Thom Shanker

The director of the National Security Agency, Gen. Keith B. Alexander, said in an interview that to prevent terrorist attacks he saw no effective alternative to the N.S.A.'s bulk collection of telephone and other electronic metadata from Americans. ...

[Shortage of IT talent slows march to cyber war](#)

Reuters, Peter Apps and Brenda Goh

For the governments and corporations facing increasing computer attacks, the biggest challenge is finding the right cyber warriors to fight back. Hostile computer activity from spies, saboteurs, competitors and criminals has spawned a growing indus...

Deterrence

[Russia test-fires nuclear-capable missile](#)

Agence France Presse, Unattributed

Russia said Thursday it had successfully test-fired an upgraded version of a nuclear-capable missile that entered into service in the

Soviet era and had been due to be scrapped. A defence ministry spokesman said the RS-12M Topol had hit its target ...

[Iran Nuclear Talks Pit UN Demands Against Proliferation Pact](#)

Bloomberg Businessweek, Jonathan Tirone

The political clash over Iran's nuclear program reflects an equally implacable legal conflict between treaties that both sides say back up their positions. Whether Iran has a right to enrich the uranium-235 isotope, used to generate atomic power a...

CWMD

[Search for Syrian Chemical Host Prompts Muted Global Response](#)

Global Security Newswire, Unattributed

The United States recently courted countries across Europe and the Middle East to potentially host Syrian chemical-warfare materials or their remnants, but no nation made an immediate, public leap for the opportunity, Foreign Policy magazine reporte...

[Syria chemical weapons: OPCW plea for short ceasefires](#)

BBC News, Unattributed

The head of the body tasked with destroying Syria's chemical weapons says fighting is preventing access to sites through some rebel-held areas. Ahmet Uzumcu, of the Organisation for the Prohibition of Chemical Weapons, called for local, short-term ...

[North Korea used chemical weapons on prisoners: report](#)

The Sydney Morning Herald, Julian Ryall

North Korea is using political prisoners held in its extensive gulag network as subjects for chemical weapons tests, according to a report in the US. The allegations have been made in the most recent report on Pyongyang's chemical weapons capabilit...

Budget

[Partial government shutdown sinks veterans' hopes of guided Offutt tour](#)

Omaha World-Herald, Rick Ruggles

Close to 30 veterans of World War II bomb groups scheduled a tour of Offutt Air Force Base for Saturday afternoon, but miscommunication about the effects of the partial government shutdown shot down their plan. About 100 people, including the vete...

U.S. Strategic Command

[General in charge of nuclear missiles is fired](#)

Associated Press, Robert Burns

The Air Force fired the general in charge of its nuclear missiles on Friday, just two days after a Navy admiral with top nuclear weapons responsibilities was sacked. Both men are caught up in investigations of alleged personal misconduct, adding to ...

COMPLETE ARTICLES:

Report: NSA collecting email and IM contacts globally

USA Today, 15 Oct 2013

Melanie Eversley & Byron Acohido

The NSA is collecting email and instant messaging contacts from overseas points, reports indicate.

The National Security Agency has been collecting contacts from people's personal email address books and instant messaging accounts in an effort to detect relationships that might be crucial to government security, the Washington Post is reporting.

The agency is collecting the data from overseas points and many of the contacts belong to Americans, the Post reports.

The Post bases its report on word from senior intelligence officials and top secret documents, including a Microsoft PowerPoint presentation, provided by former NSA contractor Edward Snowden.

The majority of the contacts harvested come from Yahoo and Hotmail accounts, but others also come from Facebook, Google and unspecified other providers, the Post reports. The contacts amount to a sizeable portion of the world's email and instant messaging accounts, according to the news organization.

"You need the haystack to find the needle," the Post quotes Gen. Keith B. Alexander, NSA director, as saying in defense of the bulk collection.

No one from public affairs was available to discuss the allegations at National Security Agency headquarters in Fort Meade, Md., Monday evening.

Senior intelligence officials say such collection would be illegal if done from facilities in the United States, according to the news organization. The NSA, however, has avoided that error by intercepting contact lists from points "all over the world," one anonymous official tells the Post.

Large technology companies use data centers around the world to ease the loads on their servers in the United States, the Post reports.

A Google spokesman told USA TODAY the Internet company had not heard of the email/instant messaging program.

"We have neither knowledge of nor participation in this mass collection of webmail addresses or chat lists by the government," the company said in a statement emailed to USA TODAY.

A Microsoft spokesman said the company does not provide the government with such data.

"Microsoft does not provide any government with direct or unfettered access to our customer's data," spokesman Dominic Carr said in an email. "We would have significant concerns if these allegations about government actions are true."

Yahoo's response was similar in an emailed statement. "We are not aware of nor have we participated in the alleged mass collection of user data by the government," the statement read.

A Facebook spokesman said the company did not know of or assist with the alleged collection of contacts.

The American Civil Liberties Union called the program a breach of Americans' rights.

"Today's revelation further confirms that the NSA has relied on the pretense of 'foreign intelligence gathering' to sweep up an extraordinary amount of information about everyday Americans," Alex Abdo, staff attorney with the ACLU National Security Project, said in an email to USA TODAY. "The NSA's indiscriminate collection of information about innocent people can't be justified on security grounds, and it presents a serious threat to civil liberties," he said.

The revelations may be adding to consumer resolve not to take online privacy so blithely. Antivirus companies ESET and AVG both said consumer interest in privacy tools have been on the rise since the Snowden disclosures began.

"People are being shocked into taking action," says Jim Brock, AVG's vice president of privacy products. "People are starting to realize that they do have some measure of control and they're staring to act on that."

Stephen Cobb, a security researcher at ESET, says many consumers now realize the personal disclosures shared on social media and web apps can get tapped by government snoops.

"I'm pretty sure consumers are adjusting their online behaviors as these round of disclosures roll on, particularly in the area of use of social media," Cobb says. "None of these revelations have had a positive impact on how people view the Internet and technology."

The silver lining may be more consumer support for online services that do a better job of respecting consumer privacy, akin to Europe's approach of giving consumers much more control over their online personas.

"People are starting to understand what this means to them, and that's good," says Brock. "It's time to move from shock and awe to taking more responsibility for our own data and doing a better job at being our own data stewards."

Defense networks vulnerable to cyberattack: Expert

CNBC, 11 Oct 2013

Jennifer Schlesinger

The U.S. government shutdown that began Oct. 1 leaves cybersecurity experts fearing the Department of Defense's computer networks may be more at risk. While Democrats and Republicans continue to battle it out, foreign adversaries may be taking advantage of the shutdown.

"Military systems are growing more complex and more intertwined daily, making them more vulnerable and on top of that, we have these ongoing issues with budgets. There was first the sequester, which cut deep into IT modernization accounts, and now there is the government shutdown," said Bob Gourley, the editor of CTOVision.com. Gourley has analyzed the U.S. military's security, including working on the most recent Defense Science Board report.

The full economic impact may not be known for months, but according to Gourley, the Pentagon's cybernetworks are vulnerable, which could lead to larger problems in the future.

A Department of Defense spokesman said by e-mail that the DOD has continued maintain critical IT operations and is ready to respond to cyber incidents.

"While the shutdown has been disruptive to our mission and many civilians remain furloughed, personnel who support key missions and activities remain on duty. These missions include sustaining critical IT capabilities and maintaining our network defenses," the spokesman said.

Authorities, with good reason, are always braced for cyberbreaches. The DOD is attacked daily, and sometimes successfully.

A Department of Defense spokesman wrote in an e-mail: "We have full confidence in the integrity of the department's networks and systems upon which we conduct critical operations. Recent reports about cyber intrusions does not change that assessment."

In May, The Washington Post reported that according to a classified report issued by the Defense Science Board, Chinese hackers had access to classified weapons systems designs. The breach included missile design systems and the plans for combat ships and aircraft.

Gourley explained the very real consequences of the breaches. "If they steal our software, they can learn how to reverse engineer and create their own software to support their own weapons systems."

He further compared the breach to the U.S. funding adversary nations' military research and development.

Russia also has successfully hacked the U.S. military, according to security experts.

In 2008, attacks breached the U.S. Central Command in Afghanistan. Flash drives with malicious code were inserted into military computers. The Pentagon has not disclosed what was taken.

James Lewis, senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies, said a similar attack could have serious consequences. "If it had happened in a war, we would have lost," he wrote in an email.

Hackers upped the ante in 2011. "In a single intrusion this March, 24,000 files were taken," former Deputy Defense Secretary William J. Lynn III said in a speech in July 2011.

For this attack, hackers targeted employees of a defense contractor.

"As long as there are humans in these enterprises, humans trying to deceive our good people, adversaries will be able to get in through this route. They send a very carefully crafted email that looks like it may come from your boss or a co-worker or someone else that you want to read," Gourley said.

When the employees opened the legitimate seeming emails, they inadvertently gave foreign hackers access to thousands of military files. The Pentagon has not disclosed what specifically was contained in the files.

N.S.A. Director Firmly Defends Surveillance Efforts

New York Times, 12 Oct 2013

David E. Sanger and Thom Shanker

The director of the National Security Agency, Gen. Keith B. Alexander, said in an interview that to prevent terrorist attacks he saw no effective alternative to the N.S.A.'s bulk collection of telephone and other electronic metadata from Americans. But he acknowledged that his agency now faced an entirely new reality, and the possibility of Congressional restrictions, after revelations about its operations at home and abroad.

While offering a detailed defense of his agency's work, General Alexander said the broader lesson of the controversy over disclosures of secret N.S.A. surveillance missions was that he and other top officials have to be more open in explaining the agency's role, especially as it expands its mission into cyberoffense and cyberdefense.

"Given where we are and all the issues that are on the table, I do feel it's important to have a public, transparent discussion on cyber so that the American people know what's going on," General Alexander said. "And in order to have that, they need to understand the truth about what's going on."

General Alexander, a career Army intelligence officer who also serves as head of the military's Cyber Command, has become the public face of the secret — and, to many, unwarranted — government collection of records about personal communications in the name of national security. He has given a number of speeches in recent weeks to counter a highly negative portrayal of the N.S.A.'s work, but the 90-minute interview was his most extensive personal statement on the issue to date.

Speaking at the agency's heavily guarded headquarters, General Alexander acknowledged that his agency had stumbled in responding to the revelations by Edward J. Snowden, the contractor who stole thousands of documents about the N.S.A.'s most secret programs.

But General Alexander insisted that the chief problem was a public misunderstanding about what information the agency collects — and what it does not — not the programs themselves.

"The way we've explained it to the American people," he said, "has gotten them so riled up that nobody told them the facts of the program and the controls that go around it." But he was firm in saying that the disclosures had allowed adversaries, whether foreign governments or terrorist organizations, to learn how to avoid detection by American intelligence and had caused "significant and irreversible damage" to national security.

General Alexander said that he was extremely sensitive to the power of the software tools and electronic weapons being developed by the United States for surveillance and computer-network warfare, and that he set a very high bar for when the nation should use them for offensive purposes.

"I see no reason to use offensive tools unless you're defending the country or in a state of war, or you want to achieve some really important thing for the good of the nation and others," he said.

Those comments were prompted by a document in the Snowden trove that said the United States conducted more than 200 offensive cyberattacks in 2011 alone. But American officials say that in reality only a handful of attacks have been carried out. They say the erroneous estimate reflected an inaccurate grouping of other electronic missions.

But General Alexander would not discuss any specific cases in which the United States had used those weapons, including the best-known example: its years-long attack on Iran's nuclear enrichment facility at Natanz. To critics of President Obama's administration, that decision made it easier for China, Iran and other nations to justify their own use of cyberweapons.

General Alexander, who became the N.S.A. director in 2005, will retire early next year. The timing of his departure was set in March when his tour was extended for a third time, according to officials, who said it had nothing to do with the surveillance controversy spawned by the leaks. The appointment of his successor is likely to be a focal point of Congressional debate over whether the huge infrastructure that was built during his tenure will remain or begin to be restricted.

Senator Patrick J. Leahy, a Vermont Democrat who leads the Senate Judiciary Committee, has already drafted legislation to eliminate the N.S.A.'s ability to systematically obtain Americans' calling records. And Representative Jim Sensenbrenner, a Wisconsin Republican and co-author of the Patriot Act, is drafting a bill that would cut back on domestic surveillance programs.

General Alexander was by turns folksy and firm in the interview. But he was unapologetic about the agency's strict culture of secrecy and unabashed in describing its importance to defending the nation.

He insisted that it would have been impossible to have made public, in advance of the revelations by Mr. Snowden, the fact that the agency collected what it calls the "business records" of all telephone calls, and many other electronic communications, made in the United States. The agency is under rules preventing it from investigating that so-called haystack of data unless it has a "reasonable, articulable" justification, involving communications with terrorists abroad, he added.

But he said the agency had not told its story well. As an example, he said, the agency itself killed a program in 2011 that collected the metadata of about 1 percent of all of the e-mails sent in the United States. "We terminated it," he said. "It was not operationally relevant to what we needed."

However, until it was killed, the N.S.A. had repeatedly defended that program as vital in reports to Congress.

Senior officials also said that one document in the Snowden revelations, an agreement with Israel, had been misinterpreted by those who believed that it meant the N.S.A. was sharing raw intelligence data on Americans, including the metadata on phone calls. Officials said the probability of American content in the shared data was extremely small.

General Alexander said that confronting what he called the two biggest threats facing the United States — terrorism and cyberattacks — would require the application of expanded computer monitoring. In both cases, he said, he was open to much of that work being done by private industry, which he said could be more efficient than government.

In fact, he said, a direct government role in filtering Internet traffic into the United States, in an effort to stop destructive attacks on Wall Street, American banks and the theft of intellectual property, would be inefficient and ineffective.

"I think it leads people to the wrong conclusion, that we're reading their e-mails and trying to listen to their phone calls," he said.

Although he acknowledged that the N.S.A. must change its dialogue with the public, General Alexander was adamant that the agency adhered to the law.

"We followed the law, we follow our policies, we self-report, we identify problems, we fix them," he said. "And I think we do a great job, and we do, I think, more to protect people's civil liberties and privacy than they'll ever know."

[Back to top](#)

Shortage of IT talent slows march to cyber war

Reuters, 13 Oct 2013

Peter Apps and Brenda Goh

For the governments and corporations facing increasing computer attacks, the biggest challenge is finding the right cyber warriors to fight back.

Hostile computer activity from spies, saboteurs, competitors and criminals has spawned a growing industry of corporate defenders who can attract the best talent from government cyber units.

The U.S. military's Cyber Command is due to quadruple in size by 2015 with 4,000 new personnel while Britain announced a new Joint Cyber Reserve last month. From Brazil to Indonesia, similar forces have been set up.

But demand for specialists has far outpaced the number of those qualified to do the job, leading to a staffing crunch as talent is poached by competitors offering big salaries.

"As with anything, it really comes down to human capital and there simply isn't enough of it," says Chris Finan, White House director for cyber security from 2011-12, who is now a senior fellow at the Truman National Security Project and working for a start-up in Silicon Valley.

"They will choose where they work based on salary, lifestyle and the lack of an interfering bureaucracy and that makes it particularly hard to get them into government."

Cyber attacks can be expensive: one unidentified London-listed company incurred losses of 800 million pounds (\$1.29 billion) in a cyber attack several years ago, according to the British security services.

Global losses are in the range of \$80 billion to \$400 billion a year, according to research by the Washington-based Center for Strategic and International Studies that was sponsored by Intel Corp's McAfee anti-virus division.

There is a whole range of attacks. Some involve simply transferring money, but more often clients' credit card details are stolen. There is also intellectual property theft or theft of commercially sensitive information for business advantage.

Victims can also suffer a "hacktivist" attack, such as a directed denial of service to bring a website down, which can cost a lot of money to fix.

Quantifying the exact damage is almost impossible, especially when secrets and money are not the only targets.

While no government has taken responsibility for the Stuxnet computer virus that destroyed centrifuges at Iran's Natanz uranium enrichment facility, it was widely reported to have been a U.S.-Israeli project.

Britain says it blocked 400,000 advanced cyber threats to the government's secure intranet last year while a virus unleashed against Saudi Arabia's energy group Aramco, likely to be the world's most valuable company, destroyed data on thousands of computers and put an image of a burning American flag onto screens.

Most cyber expertise remains in the private sector where companies are seeing an steep increase in spending on security products and services.

Depending on the cyber threat, a variety of firms are bidding for cyber talent. Google is currently advertising 129 IT security jobs, while defense companies such as Lockheed Martin Corp and BAE Systems are looking to hire in this area.

Anti-virus maker Symantec Corp is also doing good business. "The threat environment is exploding," Chief Executive Steve Bennett told Reuters in an interview in July.

The perception of an increased threat, has also led to explosive demand for the best talent.

The U.S. Bureau of Labour Statistics says the number of Information Technology security roles in the U.S. will increase by some 22 percent in the decade to 2020, creating 65,700 new jobs. Experts say it is a similar situation globally, with salaries often rising 5-7 percent a year.

"Recruitment and retention in cyber is a challenge for everybody working in this area," says Mike Bradshaw, head of security and smart systems at Finmeccanica IT unit Selex. "It's an area where demand exceeds supply ... it's going to take a while for supply to catch up."

A growing number of security firms - such as UK-based Protection Group International (PGI) - now also offer cyber services. PGI started out providing armed guards to protect merchant ships against pirates but has now hired former staff from Britain's GCHQ eavesdropping agency.

A graduate with a good computer studies degree can walk into a \$100,000 salary with a similar amount upfront as a golden handshake, several times what the U.S. National Security Agency would be likely to offer.

Western universities turn out far too few graduates with the necessary computer skills while some students complain that many of the courses on offer are too theoretical for the challenges of cyber warfare.

But applicants need not have a computer science degree to get lucrative jobs as long as they can do the hardest-to-fill jobs such as finding bugs in software, identifying elusive infections and reverse engineering computer viruses that are found on computers, said Alan Paller, founder of the non-profit SANS Institute in Washington.

SANS has worked with officials in Illinois, Massachusetts, New Jersey and other states to sponsor hacking contests that test skills in those and other areas. Educational background does not necessarily help in these contests.

Those who have "very good" skills in the most-needed areas can earn \$110,000 to \$140,000, while the very top get paid as much as \$200,000 in private sector jobs, according to Paller.

While the private sector offers big cash, the government is still able to retain some talent by appealing to people's sense of public service and patriotism.

"I want to serve my country. What I am doing is important," one hacker who conducts classified research for the U.S. military told Reuters at the Def Con hacking conference in July. He declined to provide his name because he was not authorized to speak to the press.

There is also an expectation that government workers can move to more lucrative jobs in the private sector after several years in public service.

But some senior officers in Western militaries still fear they may struggle to attract the requisite talent, citing both cultural and administrative problems.

General Keith Alexander, head of both the NSA and Cyber Command, told Reuters earlier this year finding the right talent was a priority. He has attended events such as the Def Con hacker conference, trading his uniform for a black T-shirt.

Hiring outsiders has long been thought to be a tactic employed by the United States as well as China and Russia.

Western security officials believe Russia, China and other emerging cyber powers such as Iran and North Korea have cut deals with their own criminal hacker community to borrow their expertise to assist with attacks.

Russia and China, which have been accused by the West of mounting repeated attacks on government and commercial interests, deny direct involvement in hacking.

"We are at the very beginning of this process and we are building it brick by brick," says Colonel Gregory Conti, head of the cyber Security Department at the U.S. Military Academy, West Point. "It's going to be like the creation of the air force - a process of several decades getting the right people and structures." (\$1 = 0.6209 British pounds)

[Back to top](#)

Russia test-fires nuclear-capable missile

Agence France Presse, 10 Oct 2013

Unattributed

Russia said Thursday it had successfully test-fired an upgraded version of a nuclear-capable missile that entered into service in the Soviet era and had been due to be scrapped.

A defence ministry spokesman said the RS-12M Topol had hit its target at a test range that Russia leases from Kazakhstan after it was fired from the Kapustin Yar military site near the Caspian Sea.

"The exercise head of the rocket hit the hypothetical target on the Sary-Shagan test site in Kazakhstan," spokesman Igor Yegorov told the Interfax news agency.

Russia is the only country in the world to still test-launch intercontinental ballistic missiles. Most of the launches are performed to either ensure the safety of Russia's ageing arsenal or to test new rockets that could penetrate a missile defence system now gradually being deployed by NATO in Europe.

Yegorov said the launch was designed to test improvements meant to keep the RS-12M Topol - a three-stage ballistic missile that has provided the backbone of Russian defences since Soviet times - in service for years to come.

"The purpose of this launch was to confirm the stability of the main flight parameters of this class of rocket during extended service," Yegorov said.

Yegorov said the first RS-12M Topol entered into service 25 years ago.

[Back to top](#)

Iran Nuclear Talks Pit UN Demands Against Proliferation Pact

Bloomberg Businessweek, 13 Oct 2013

Jonathan Tirone

The political clash over Iran's nuclear program reflects an equally implacable legal conflict between treaties that both sides say back up their positions.

Whether Iran has a right to enrich the uranium-235 isotope, used to generate atomic power and make nuclear bombs, is at the heart of a dispute that has raised the specter of war for the past decade. The primacy of the question may be the only area of agreement this week in the first round of international talks since Hassan Rouhani was elected Iran's president on a pledge to resolve the dispute.

"The question of enrichment is at the center of the negotiations themselves," U.S. Secretary of State John Kerry said Oct. 10 in Kuala Lumpur. "I've personally had private discussions with the foreign minister and I think it's best to keep those discussions private and personal at this point."

Iran asserts the right to enrich uranium under the 1968 Nuclear Non-Proliferation Treaty, an interpretation rejected by the United Nations Security Council, which says its demands take precedence. While Iran says its nuclear work under international monitors is peaceful, its past deceptions and alleged military work have compelled the UN to order a suspension of enrichment. It has imposed four rounds of sanctions aimed at undermining the country's economy and restricting its access to nuclear technology.

"The obligations imposed by the UN Charter trump any inconsistent treaty, including the Nuclear Non-Proliferation Treaty," Michael Glennon, an international-law professor at Tufts University near Boston, said in an e-mail. Challenging the legality of the UN's actions "at this point would be diplomatic suicide," said Glennon, who has advised UN atomic monitors and the U.S. State Department.

The Geneva talks, scheduled for Oct. 15 and 16, will include China, France, Germany, Russia and the U.K., in addition to the U.S. The senior U.S. official will be Under Secretary of State for Political Affairs Wendy Sherman and Iran will be represented by Foreign Minister Mohammad Javad Zarif.

Iran, with enough enriched uranium to make 15 atomic weapons if it chooses, has called the sanctions illegal. It insists the 1968 NPT is the legal standard by which its rights should be measured. The treaty allows signatories access to peaceful nuclear technologies in exchange for a pledge they won't use that expertise to develop weapons.

Iran won't ship out any of its stockpile of enriched uranium, Abbas Araghchi, deputy foreign minister said on state TV today. "We will negotiate about the form, size and level of enrichment, but transporting the enriched stockpile out of the country is one of our red lines," Araghchi said.

Other countries, including those that have had nuclear weapons programs like Brazil and South Africa, enrich uranium. Iran denies its military had a role in nuclear work and questions why it shouldn't have the same rights.

Iran will put forward a three-step proposal at the talks, according to the Iranian Students News Agency. As part of the plan, Iran would seek a commitment from the so-called P5+1 to recognize the country's right to enrich at the end of the talks.

"The essence of the matter is that many similarly situated NPT non-nuclear weapon states have uranium-enrichment programs," Dan Joyner, a University of Alabama law professor who wrote the book "Interpreting the Nuclear Non-Proliferation Treaty," said in an e-mail. "The UN resolutions calling for Iran to cease uranium enrichment were ill-considered, and arguably exceeded the authority of the Security Council."

Rouhani, who negotiated a two-year suspension of Iran's nuclear work from 2003 to 2005, has invoked Pakistan and Brazil as examples for Iran.

"The world did not want Pakistan to have an atomic bomb or Brazil to have the fuel cycle, but Pakistan built its bomb and Brazil has its fuel cycle, and the world started to work with them," he said in a 2004 speech to Iran's Supreme Cultural Revolution Council, according to reproduced text from his talk published by Brandeis University in Waltham, Massachusetts. "Our problem is that we have not achieved either one, but we are standing at the threshold."

Brazil, with the world's No. 5 uranium reserves, abandoned decades of covert work in the early 1990s while keeping its enrichment program for domestic energy needs. South Africa, which had atomic devices during the apartheid era, has plans to expand its

enrichment program, according to the South African Institute of International Affairs in Johannesburg.

[Back to top](#)

Search for Syrian Chemical Host Prompts Muted Global Response

Global Security Newswire, 11 Oct 2013

Unattributed

The United States recently courted countries across Europe and the Middle East to potentially host Syrian chemical-warfare materials or their remnants, but no nation made an immediate, public leap for the opportunity, Foreign Policy magazine reported on Thursday.

At least one plan calls for all but the deadliest materials in the Syrian government's chemical arsenal to be eliminated outside the nation's borders. However, locations for the planned destruction effort remained unclear, as did the ultimate destinations of its by-products.

A largely U.S.-led search for destruction assistance included contacts with Albania, Belgium, France and Russia, which all have historical experience in destroying chemical-weapon stocks. U.S. officials also reached out to Norway, which has no history in dealing with such substances.

One chemical-weapon expert said he was "surprised" by the latter inquiry.

"The best option is to destroy the chemicals and the precursors on-site in Syria. That would seem better than approaching a country like Norway," said Paul Walker, international program director of the environmental security and sustainability program of Green Cross and Global Green.

The Syrian government admitted possessing chemical weapons and agreed to their destruction about a month ago, after an August nerve-gas attack prompted an immediate threat of U.S. military intervention in the country's civil war. The agreement kicked off a whirlwind disarmament effort resulting in Friday's Nobel Peace Prize award to the international agency charged with counting and overseeing elimination of the Syrian stocks.

An eight-month push to corral and destroy the arms will involve "exceedingly complex security challenges related to ensuring a safe operating environment at destruction sites," U.N. Secretary Ban Ki-moon said in a Monday planning document. The U.N. Security Council later signed off on the U.N. chief's proposal, the Associated Press reported on Friday.

What equipment would destroy the materials also remains uncertain. The U.S. Defense Department on Tuesday described a recently developed, portable disposal system to the Organization for the Prohibition of Chemical Weapons, which has until Nov. 15 to settle on specific gear, Reuters reported.

"This is very big business, very political, and several governments are pushing for it," said Dieter Rothbacher, a former OPCW personnel trainer.

A spasm of Thursday violence near a reported chemical-arms site underscored security risks to the international disarmament effort, the Wall Street Journal reported.

Backers of the Syrian resistance said the stepped-up fighting took place near the Safira Defense Factories and Scientific Research Facilities. A number of specialists said the Safira installation -- a reported laboratory and manufacturing site -- is among the country's most sizable and cutting-edge.

Moscow, an ally of Syrian President Bashar Assad, reaffirmed its contention that the opposition is engaged in chemical-warfare activities, state-run Russia Today reported on Friday.

"Some reports indicate that [the] al-Nusra Front is planning to smuggle toxic compounds and relevant specialists into Iraqi territory to stage terrorist attacks there this time," Russian Foreign Minister Sergei Lavrov said.

Lavrov added that operatives from outside governments might have given related training to Syrian opposition fighters in tribal territories of Afghanistan. The Russian media report did not identify what countries could have contributed.

[Back to top](#)

Syria chemical weapons: OPCW plea for short ceasefires

BBC News, 14 Oct 2013

Unattributed

The head of the body tasked with destroying Syria's chemical weapons says fighting is preventing access to sites through some rebel-held areas.

Ahmet Uzumcu, of the Organisation for the Prohibition of Chemical Weapons, called for local, short-term ceasefires to allow experts to work.

Syria officially joined the Chemical Weapons Convention on Monday.

Meanwhile, three of the six Red Cross workers who were kidnapped on Sunday have been freed, the ICRC has said.

A Syrian Red Crescent volunteer who was with them has also been released, the group added. All those freed are reported to be unharmed.

The seven workers were seized near the town of Saraqeb in Idlib province, where they were delivering aid and assessing health facilities. It is not clear who carried out the kidnapping.

The OPCW and the UN have had a team of 60 experts and support staff in Syria since 1 October. They are based in Damascus and have been carrying regular visits to facilities.

In his first interview since the OPCW won the Nobel Peace Prize last week, Mr Uzumcu told the BBC's Today programme that Syrian officials had been co-operating and facilitating the experts' work.

He said they had been taken wherever they wanted to go, and that they had already reached five out of at least 20 facilities capable of producing chemical weapons.

However, Mr Uzumcu said, routes to some of the sites went through opposition-held territory and this prevented access.

"They change hands from one day to another, which is why we appeal to all sides in Syria to support this mission, to be co-operative and not render this mission more difficult. It's already challenging," he said.

He said he had called for truces because "in the previous, UN-led mission to investigate allegations of use [of chemical weapons] there were temporary ceasefires of four or five hours which helped this mission".

He added that one abandoned site was located in a rebel-held area, and that his team was hoping to access it. It is the first time the OPCW has worked in a war zone since it was set up in 1997.

Mr Uzumcu also said that on Saturday mortar shells had fallen "next to the hotel where our team is staying and there are exchanges of fire not far from where they go".

Details of the visits have not been released. Syria is believed to possess mustard gas, as well as the sarin and VX nerve agents.

Meanwhile, US Secretary of State John Kerry has said a peace conference should be held in Geneva as soon as possible to set up an interim government.

"There has to be a transition government in Syria to permit the possibility of peace," he said.

The dominant group in the main opposition alliance, the Syrian National Council, has said it will not take part in the proposed peace negotiations - known as Geneva II.

In his interview with the BBC, Mr Uzumcu said the Nobel prize had been a "very big boost" to the morale of his teams. "They are working in very challenging circumstances in the field," he said.

The OPCW, based in The Hague, was established to enforce the 1997 Chemical Weapons Convention. Its main role to monitor and destroy chemical weapons.

The disarmament deal on Syria's chemical weapons was sparked by a poison-gas attack in Damascus on 21 August in which hundreds were killed. Western nations blamed the forces of President Bashar al-Assad, but he blamed rebel fighters.

Syria later agreed to join the global Chemical Weapons Convention, and the UN said it would bound by the treaty from 14 October.

Under a UN resolution, Syria's chemical weapons production equipment must be destroyed by 1 November and stockpiles must be disposed of by mid-2014.

Violence in the country is continuing. On Monday a car bomb killed at least 12 people in the north-western rebel-held town of Darkoush in Idlib province, activists say.

The attack came a day after seven workers of the International Committee of the Red Cross were abducted near Saraqeb, a town also located in Idlib province, near the Turkish border.

Syrian state TV blamed rebels for the abduction.

[Back to top](#)

North Korea used chemical weapons on prisoners: report

The Sydney Morning Herald, 15 Oct 2013

Julian Ryall

North Korea is using political prisoners held in its extensive gulag network as subjects for chemical weapons tests, according to a report in the US.

The allegations have been made in the most recent report on Pyongyang's chemical weapons capabilities by 38 North, the respected website operated by the US-Korea Institute at Johns Hopkins School of Advanced International Studies, and are based on testimony from both prisoners and former guards who managed to defect.

One defector who served as a security official at Detention Camp 22 described tests in which healthy prisoners were placed inside glass chambers and technicians monitored the effects as gas was pumped into the chambers.

"Normally, a family sticks together and individual prisoners stand separately around the corners," Kwon Kyok, a pseudonym, said in a documentary cited by the report.

"I watched a whole family being tested on suffocating gas and dying in the gas chamber: parents, one son and a daughter," he said.

"The parents were vomiting and dying, but until the very last moment they tried to save the kids by doing mouth-to-mouth breathing.

"For the first time it hit me that even prisoners are capable of powerful human affection."

A former member of the North Korean military recounted his involvement in similar experiments on an island off the west coast of the Korean peninsula. It has parallels with a report issued by a human rights group in Seoul in June that claimed the North was carrying out chemical and biological weapons experiments on disabled children on an island off South Hamgyong Province.

The report said the claims of political prisoners being used as test subjects for chemical weapons were "extremely difficult to confirm".

However, it added: "Taken as a whole, and within the context of what is currently known about the treatment of political prisoners, such reports suggest a long-standing policy of low-level lethal testing of chemical agents on unwilling human subjects."

The study suggested that North Korea was able to manufacture 4500 tonnes of chemical agents a year, but had the capacity to increase that up to 12,000 tonnes a year in the event of war.

The chemicals the regime was producing included hydrogen cyanide, phosgene, sarin, tabun, chlorine and a number of agents from the mustard gas family.

The report added that North Korea had reportedly provided chemical weapons or technology for chemical weapons to Egypt, Iran,

Libya and Syria since the 1990s.

[Back to top](#)

Partial government shutdown sinks veterans' hopes of guided Offutt tour

Omaha World-Herald, 12 Oct 2013

Rick Ruggles

Close to 30 veterans of World War II bomb groups scheduled a tour of Offutt Air Force Base for Saturday afternoon, but miscommunication about the effects of the partial government shutdown shot down their plan.

About 100 people, including the veterans and their spouses, children and grandchildren from around the United States, attended the annual reunion in Omaha of the 461st and 484th Bombardment Groups.

Ryan Hansen, a spokesman for the 55th Wing at Offutt, said the veterans could have taken an unguided tour.

"We're not sure what the disconnect was," Hansen said. "It's unfortunate. We were looking forward to having them out."

Participants in the four-day reunion visited Boys Town, Mahoney State Park, the Strategic Air & Space Museum and Durham Museum. But the veterans, men who flew missions in B-24 bombers through heavy flak over Germany, Italy and other countries, were eager to take a bus tour of Offutt.

Mick Bloom of Bellevue, an 88-year-old who was a gunner in the 484th Bombardment Group, said he confirmed the Offutt tour through base personnel on Monday. "Two hours later they called me at home and told me it's all canceled," Bloom said.

Bloom said Offutt representatives told him the tour couldn't take place because of the partial government shutdown, even though the veterans had their own chartered buses. Bloom said it was his understanding that Offutt volunteers had been ready to guide them.

Hansen said 55th Wing leadership received permission late last week to allow the bomb-group veterans to take an unguided tour with no federal resources utilized. Offutt officials left a message or messages for Bloom, Hansen said, to inform the veteran of this development but didn't hear back from him.

Bloom said he left for the reunion Thursday and didn't receive the message.

Hansen also said the guides Bloom envisioned weren't volunteers but were public affairs staffers at the base and thus wouldn't have been able to guide the tour because of the partial shutdown. Bloom said he doubted he could have lined up excellent guides who knew base history and other facts and figures.

The 461st and 484th bomb groups shared an airfield in Italy during World War II. They have held joint reunions in the Midwest over the past three years, said Hughes Glantzberg of Gunnison, Colo.

Glantzberg's father, Frederic, was commanding officer of the 461st. Hughes Glantzberg is president of the 461st Bombardment Group Association.

The men spoke about their frustration Saturday before going into the Durham Museum. The Offutt visit was to take place later in the afternoon.

Bloom didn't blame Offutt personnel. He said they had orders from way above them.

"We planned this thing so far in advance," Bloom said. "The people at Offutt are disappointed."

Hansen said it's important to him and his colleagues that veterans get appropriate support. The last thing he wanted, he said, was to disappoint them.

[Back to top](#)

General in charge of nuclear missiles is fired

Associated Press, 11 Oct 2013

Robert Burns

The Air Force fired the general in charge of its nuclear missiles on Friday, just two days after a Navy admiral with top nuclear weapons responsibilities was sacked. Both men are caught up in investigations of alleged personal misconduct, adding to a cascade of turmoil inside the nation's nuclear weapons force.

The Air Force removed Maj. Gen. Michael Carey, a 35-year veteran, from his command of 20th Air Force, responsible for all 450 of the service's intercontinental ballistic missiles. Carey, who took his post in Wyoming in June 2012, will be reassigned pending the outcome of an investigation into personal misbehavior, the service said.

The Air Force would not specify what Carey is alleged to have done wrong, but two officials with knowledge of the investigation indicated that it was linked to alcohol use.

They said it was not related to the performance or combat readiness of ICBM units or to his stewardship of the force.

Removing senior officers in the nuclear force is rare but has happened twice this week.

On Wednesday the Navy said Vice Adm. Tim Giardina, the second-in-charge at U.S. Strategic Command, was fired amid an investigation of gambling issues. He was demoted from three- to two-star rank and reassigned to a Navy staff job until the investigation is completed.

Together, the Carey and Giardina firings add a new dimension to a set of serious problems facing the military's nuclear force. The ICBM segment in particular has had several recent setbacks, including a failed safety and security inspection at a base in Montana in August, followed by the firing of the colonel there in charge of security forces. In May, The Associated Press revealed that 17 Minuteman 3 missile launch control officers at Minot Air Force Base, N.D., had been taken off duty in a reflection of what one officer there called "rot" inside the ICBM force.

Air Force Gen. Robert Kehler, the nation's most senior nuclear commander as head of U.S. Strategic Command, called the Carey and Giardina matters "unfortunate behavioral incidents," but he would not discuss details.

In a telephone interview from his headquarters near Omaha, Neb., Kehler said he told Secretary of Defense Chuck Hagel and the chairman of the Joint Chiefs of Staff, Army Gen. Martin Dempsey, on Thursday that the two cases had not shaken his confidence in the force.

"I still have 100 percent confidence that the nation's nuclear deterrent force is safe, secure and effective." He added that "this is something that has been on their minds as well," referring to Hagel and Dempsey.

"You are going to have to make your own judgment when all the facts come out on these two particular cases, but I can say this: In these cases, this ultimately had to do with a loss of confidence" in Carey and Giardina "as a result of certain behavior."

Other problems have surfaced this year. In a March inspection, launch crews at Minot scored the equivalent of a "D" grade on missile operations. In June the Minot officer in charge of training and proficiency of missile crews was fired.

Throughout this period the Air Force and top Pentagon officials have insisted that the nuclear force is safe and secure. But the competence of its management has been questioned.

Documents obtained by the AP show that at lower levels the force is beset with morale problems and incidents of indiscipline.

The U.S. has been shrinking the size of its nuclear arsenal for many years; it is comprised of long-range missiles aboard submarines, long-range bombers and ICBMs. As of Oct. 1 the U.S. had 1,688 deployed strategic nuclear warheads, which Washington is obliged to reduce to 1,550 by 2018 under the New START treaty with Russia.

As the arsenal has grown smaller, questions about management of the force have loomed larger. Rep. Howard "Buck" McKeon, the Republican chairman of the House Armed Services Committee, said in August that the Air Force must refocus on its nuclear mission. He urged it to "hold failed leadership" accountable and to "recommit itself from the top down" to the mission of safely operating nuclear weapons.

The decision to sack Carey was made by Lt. Gen. James Kowalski, commander of Air Force Global Strike Command, which is in charge of all Air Force nuclear weapons, including bombers. The case appears to be unrelated to that of Giardina, but the two men

are associated in the chain of responsibility for U.S. nuclear weapons.

Carey did not report directly to Giardina, but the ICBMs under Carey's command would, in the event of war, receive their launch commands through Strategic Command, where Giardina had been the deputy commander since December 2011. By coincidence, Kowalski, who fired Carey, has been nominated to succeed Giardina at Strategic Command. The Senate has not yet confirmed Kowalski.

Kowalski selected the vice commander of Air Force Global Strike Command, Maj. Gen. Jack Weinstein, to temporarily replace Carey.

"It's unfortunate that I've had to relieve an officer who's had an otherwise distinctive career spanning 35 years of commendable service," Kowalski said in a written statement from his headquarters at Barksdale Air Force Base, La.

An internal email obtained by the AP on Friday said the allegations against Carey stem from an inspector general probe of his behavior while on an unspecified "temporary duty assignment." The email said the allegations are not related to the operational readiness of the ICBM force or recent failed inspections of ICBM units.

At a Pentagon news conference, an Air Force spokesman, Brig. Gen. Les Kodlick, would not provide details about the alleged misbehavior by Carey except to say it does not involve sexual misconduct or criminal activity. He said the investigation had been underway for several months.

"There was misbehavior such that (Kowalski) decided that it didn't exemplify the trust and responsibilities required of a commander who is responsible for the nuclear force," Kodlick said.

"Especially in the nuclear enterprise, it's a position of great trust and responsibility. The nuclear deterrence mission is one of great focus, discipline. Personal behavior is vital to that, especially from a commander."

Separately, two senior defense officials with knowledge of the allegations told the AP that they are at least partly related to alcohol use. The officials spoke only on condition of anonymity because they were not authorized to discuss an internal investigation that is not yet finished.

Carey began his Air Force career in the enlisted ranks in 1978. He was commissioned as an officer in 1983 and is a veteran of the wars in Iraq and Afghanistan. He took command of the ICBM force, at 20th Air Force headquarters at F.E. Warren Air Force Base, Wyo., in June 2012.

[Back to top](#)