

P3/b(3)

50 USC 3507

Sent: Wed, 27 Oct 2010 04:27:28 -0400

From: [REDACTED]

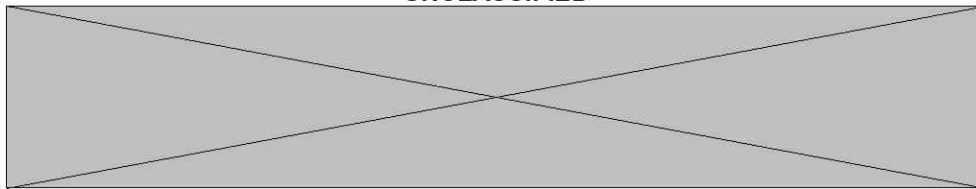
To: wloehrs@pfiab.eop.gov, "Martinsson, Charlotte K." <charlotte_k._martinsson@pfiab.eop.gov>, "Osburn, Stefanie" <stefanie_r._osburn@pfiab.eop.gov>

Cc: [REDACTED]

Subject: Mobile Version -- Media Highlights for Wednesday, 27 October 2010

[Mobile Version.htm](#)

P6/b(6)



27 October 2010

Produced by the CIA Office of Public Affairs

COPYRIGHT NOTICE

The material contained in Media Highlights may be subject to copyright. Further reproduction or dissemination by any means is subject to original copyright restrictions and is generally prohibited without the copyright holder's permission. This publication is intended to assist employees in their official capacities. It is not a replacement for commercial publications or services, but rather a tool for highlighting issues of particular importance to the mission of the Central Intelligence Agency.

Terrorism

[1. BLOG: 'The Blotter' -- American Al Qaeda May Now Pose Most Clear Threat to Homeland Security](#)

U.S. Authorities Worry Over Americans Rising to Leadership Roles in Al Qaeda

Pierre Thomas, Jack Cloherty and Jason Ryan, ABCNews.com, 26 October 2010

[2. American arrested in terrorism case was denied entry to Pakistan](#)

New York-born Abdel Hameed Shehadeh had tried unsuccessfully to travel to Pakistan, Jordan and Somalia, and he was rejected by the Army. Authorities arrested him last week in Honolulu, where he had been taking target practice.

Richard A. Serrano, Los Angeles Times, 27 October 2010

Cybersecurity Issues

[3. Hackers shopping malware network](#)

Suspected of backing Iran

Shaun Waterman, Washington Times, 27 October 2010

[4. Republican Aides Say Cybersecurity Bill Will Wait for Next Year](#)

Tim Starks, CQ.com, 26 October 2010

[5. Cyber Threat to DHS Networks Continues to Grow](#)

Rob Margetta, CQ.com, 26 October 2010

Detainee Issues

[6. Republicans Probe Gitmo Transfers to Europe](#)

Evan Perez, Wall Street Journal, 27 October 2010, Page A6

[7. Psychiatrist: Detainee is 'highly dangerous'](#)

In the sentencing phase of Omar Khadr's teen terror case, a forensic psychiatrist called the Canadian devout and angry.

Carol Rosenberg, Miami Herald, 27 October 2010

[8. Candid Talks by Detainee Were Caught on U.S. Tapes](#)

Benjamin Weiser, New York Times, 27 October 2010, Page A25

[9. Terror suspect held at CIA secret prison gets victim status in Polish probe](#)

Adam Goldman and Vanessa Gera, Associated Press, LATimes.com, 27 October 2010

Wikileaks Document Release

[10. U.S. Military Sees Additional Document Leaks Ahead](#)

Julian E. Barnes and Joe Lauria, Wall Street Journal, 27 October 2010, Page A24

[11. U.S.: Enemies Searching WikiLeaks Iraq Papers](#)

Lara Jakes, Associated Press, Time.com, 26 October 2010

[12. WikiLeaks has more US war files, Pentagon says](#)

** WikiLeaks threatens to release more Afghan war documents*

** Group already has released 500,000 US Iraq, Afghan files*

Phil Stewart, Reuters.com, 26 October 2010

[13. In Information Age, Leaks Are Here To Stay](#)

Tom Gjelten, NPR.org, 26 October 2010

Middle East/South Asia

[14. Taliban unscathed by U.S. strikes](#)

Greg Miller, Washington Post, 27 October 2010, Page A1

[15. Afghan aid spent with little local input, audit finds](#)

Karen DeYoung, Washington Post, 27 October 2010, Page A14

[16. Afghan security problem: Poorly built police stations](#)

Marisa Taylor and Warren P. Strobel, McClatchyDC.com, 26 October 2010

[17. Russia could play big role in Afghanistan after talks with Nato](#)

Deborah Haynes, The Times, UK, 27 October 2010

[18. U.S. Tries Restart of Talks With Iran](#)

Jay Solomon, Wall Street Journal, 27 October 2010, Page A1

[19. Iran Begins Loading Fuel at Nuclear Reactor](#)

William Yong and Alan Cowell, New York Times, 27 October 2010, Page A8

[20. Teenage Recruit Joins Jihad](#)

Would-Be Suicide Bomber in Karachi Tells of Pakistan Taliban Indoctrination

Tom Wright and Owais Tohid, Wall Street Journal, 27 October 2010, Page A15

[21. Saudi Border With Yemen Is Still Inviting for Al Qaeda](#)

Robert F. Worth, New York Times, 27 October 2010, Page A1

[22. Yemeni journalist on trial for Qaeda, Awlaki links](#)

** Shai accused of trying to recruit for al Qaeda*

** Defence lawyers boycott trial*

Reuters.com, 26 October 2010

[23. In Mideast House of Cards, U.S. Views Lebanon as Shaky](#)

Mark Landler, New York Times, 27 October 2010, Page A4

[24. Turkey in Dilemma Over NATO Shield](#)

Marc Champion, Wall Street Journal, 27 October 2010, Page A13

Iraq

[25. Iraq al Qaeda more lethal as homegrown insurgency](#)

Suadad Al-salhy, Reuters.com, 26 October 2010

[26. Saddam aide Tariq Aziz sentenced to death in Iraq](#)

Two others face same fate for persecution, murder

Ashish Kumar Sen, Washington Times, 27 October 2010

[27. Anbar Province, Once a Hotbed of Iraqi Insurgency, Demands a Say on Resources](#)

John Leland and Khalid D. Ali, New York Times, 27 October 2010, Page A10

Russia/Europe

[28. Urban terror threats prompt new UK police training](#)

Paisley Dodds, Associated Press, FederalNewsRadio.com, 26 October 2010

[29. In Russia, corruption has taken on a life of its own](#)

Will Englund, Washington Post, 27 October 2010, Page A12

[30. Gorbachev Says Putin Obstructs Democracy](#)

Clifford J. Levy, New York Times, 27 October 2010, Page A8

[31. Europe amplifies objections to U.S. data-sharing system](#)

Edward Cody, Washington Post, 27 October 2010, Page A13

Latin America/Africa

[32. Chavez orders takeover of Owens-Illinois branch](#)

Ian James, Associated Press, FederalNewsRadio.com, 26 October 2010

Obituaries

[33. William Broe, former high-level CIA official, dies at 97](#)

T. Rees Shapiro, Washington Post, 26 October 2010

Opinion

[34. The Online Threat](#)

Should we be worried about a cyber war?

Seymour M. Hersh, The New Yorker, 1 November 2010

[35. The Demographic Future](#)

What Population Growth – and Decline – Means for the Global Economy

Nicholas Eberstadt, Foreign Affairs, November/December 2010

[36. Can the CIA still accomplish its mission?](#)

Charles Faddis, CNN.com, 26 October 2010

Other

[37. SpyTalk: NYU gets the papers of Philip Agee, renegade CIA agent](#)

38. U.S. Lost Communications With 50 Nukes

39. FBI links shots fired at Pentagon, Marine museum

[Back To Table Of Contents](#)

UNCLASSIFIED

1. BLOG: 'The Blotter' -- American Al Qaeda May Now Pose Most Clear Threat to Homeland Security

U.S. Authorities Worry Over Americans Rising to Leadership Roles in Al Qaeda

Pierre Thomas, Jack Cloherty and Jason Ryan, ABCNews.com, 26 October 2010

American Al Qaeda may now pose the most clear and present threat to the homeland, top government sources tell ABC News.

Americans have risen high in Al Qaeda's leadership and are now helping shape strategy for attacks on the U.S.

One source told ABC that it is clear these homegrown Al Qaeda want to spill American blood.

American Al Qaeda may be even more dangerous than foreign fighters, sources say, because they know the nation's psyche and its "soft" targets, and its American recruits can often move about the country freely. In fact, during a speech to the top police chiefs in the country Monday, Homeland Security Secretary **Janet Napolitano** shared a stark assessment:

"The stark reality that I shared with Congress recently -- and that I'm sharing with you today -- is that we at the **Department of Homeland Security**, and I venture to say the **FBI** as well, are operating under the premise that individuals prepared to carry out terrorist acts are already in the country, and may carry out these acts of violence with little or no warning," Napolitano said.

So who are these self-proclaimed traitors now in the Al Qaeda leadership? The Yemeni-American cleric Anwar Al Awlaki, once a propagandist, has now gone operational, and sources say Awlaki is emerging as a top threat to America, perhaps even enemy number one after Osama Bin Laden himself. Awlaki has ties to the Fort Hood shooter, and U.S. officials say he was a key figure behind the Christmas plot to blow-up an airplane over Detroit.

While Awlaki is known to many Americans, he is now joined by a supporting cast of radicalized, and dangerous, former Americans. Adnan Shukrijumah lived in Florida and was in the U.S. at least 15 years as a permanent resident. He is now believed to be a top Al Qaeda operational leader. The government says he helped plan a failed plot on the New York City subway system last year.

Anwar Awlaki and Shukrijumah are both believed to be actively plotting attacks right now. And sources tell ABC that Al Qaeda desperately wants another hit on the homeland before the tenth anniversary of the 9/11 attacks.

American Members of Al Qaeda Want Another Attack on U.S.

Another American Al Qaeda is Adam Gadahn, formerly of California. He's perhaps the top propagandist for Al Qaeda. Just this past weekend he used the internet to urge Muslim immigrants in the suburbs of Detroit to murder their non-Muslim neighbors.

Samir Khan lived in Queens, N.Y., and in Charlotte, N.C., but now he says, "I am proud to be a traitor to America." Sources say he is a major player behind "INSPIRE," an online Al Qaeda magazine which is aimed at radicalizing and recruiting young Muslim Americans. The magazine recently called for conducting lunch hour attacks at Washington, D.C., restaurants.

Yahya Ibrahim, a radical Egyptian cleric, allegedly penned the article that mentions this but the whole magazine is believed to be written by Khan and Awlaki.

These calls for violence fit with what senior counterterror officials have told ABC News: that American Al Qaeda are urgently pushing for its followers to launch attacks like the 2007 assault in Mumbai, India. They believe even a small scale attack, if successful, will generate international coverage and shake American confidence.

Former **FBI** official Brad Garrett says, "We would be just as traumatized if someone walked into a mall or train station then if you had another 9/11."

Counterterrorism officials are clearly warning Americans that the threat from the new American Al Qaeda is very real.

UNCLASSIFIED

2. American arrested in terrorism case was denied entry to Pakistan

New York-born Abdel Hameed Shehadeh had tried unsuccessfully to travel to Pakistan, Jordan and Somalia, and he was rejected by the Army. Authorities arrested him last week in Honolulu, where he had been taking target practice.

Richard A. Serrano, Los Angeles Times, 27 October 2010

Reporting from Washington -- Abdel Hameed Shehadeh, according to the **FBI**, traveled the world in search of jihad. But Pakistan turned him away, and Jordan did too. He tried to get into Somalia, but U.S. authorities had placed him on the no-fly list.

An American citizen, he visited an Army recruiting station in New York's Times Square hoping to be sent to Iraq; the Army did not want him either.

So, the **FBI** said, the 21-year-old born and raised in New York created websites and posted threats of radical Islamic violence, including one from another American, Anwar Awlaki, a terrorism suspect thought to be living in Yemen. Then Shehadeh flew to Hawaii and allegedly started taking target practice.

FBI agents said he wanted to join an Islamic militant group to learn "guerrilla warfare and bomb-making." Had he been welcomed into the Army, they said, his plan was to defect in Iraq and turn against his comrades.

Shehadeh's journeys ended Friday. He was arrested in Honolulu and accused in a federal criminal complaint, unsealed Monday, of making false statements in an international terrorism case.

For more than two years federal officials followed his travels, tracked his websites and enlisted help from his grade-school friends. On Tuesday, they singled him out as someone much like Awlaki - eager to forfeit his U.S. citizenship for a life of jihad.

"My brothers of revolutionary Islam, I am with you as long as you keep struggling," Shehadeh allegedly posted on his website. "Trust me there are many brothers and sisters in America that are ready to speak up. They just need a push."

Florence T. Nakakuni, the U.S. attorney in Hawaii, said the investigation covered "a six-hour time difference and 5,000 miles." In New York, **FBI** Assistant Director Janice K. Fedarcy said, "Stopping one prospective terrorist can prevent untold numbers of casualties."

Shehadeh faces up to eight years in prison. His Hawaiian attorney, Matthew Winter, said he "wants to return as soon as possible to New York and face the charges there."

He first drew the eye of **FBI** agents in June 2008 for signing into the online Expedia travel agency and purchasing a one-way ticket to Pakistan. A New York detective interviewed him at the airport; Shehadeh said he was going to Pakistan to attend an Islamic school.

Customs and Border Patrol searched his checked baggage. They found a sleeping bag, toiletries, three books and two changes of clothes. When the plane landed in Islamabad, he was not allowed into the country.

The **FBI** developed two confidential informants who were boyhood classmates of Shehadeh. He allegedly told the informants that he wanted to die a martyr and spoke of an afterlife with 72 virgins.

In June 2009, he purchased a ticket to Dubai, United Arab Emirates. Again **FBI** agents said they interviewed him; he told them his destination was Somalia. But now he was on the no-fly list; he could not even leave the U.S.

He went to Hawaii. In October 2009, he visited the SWAT Gun Club in Honolulu and practiced firing an M-16 assault rifle, .45-caliber and 9-millimeter semiautomatic pistols, and a .44-caliber Magnum revolver.

In April, he again spoke to the **FBI**. The conversation turned to why U.S. Muslims become radicalized. The agents said Shehadeh told them, "Take my story, for example."

Copyright © 2010, Los Angeles Times

[Back To Table Of Contents](#)

UNCLASSIFIED

3. Hackers shopping malware network

Suspected of backing Iran

Shaun Waterman, Washington Times, 27 October 2010

A hacker group calling itself the Iranian Cyber Army is assembling a network of infected computers, and selling it to cybercriminals to

spread spam and malicious software, according to security researchers.

Aviv Raff, of the computer security firm Seculert, told The Washington Times that the group was exploiting a vulnerability in WordPress, a popular blogging software program, to gain control of unsuspecting Internet users' computers and add them to its network -- known as a botnet, or robot network -- of infected machines. He said the botnet, one of hundreds controlled by hacker gangs and cybercrime syndicates all over the world, could be used to launch cyber-attacks against Tehran's enemies.

Most researchers regard the Iranian Cyber Army (ICA) as "hacktivists" -- politically motivated pro-Iranian hackers -- and there is no evidence they are linked to the Tehran government. Almost a year ago, a group using that name attacked U.S.-based social networking platform Twitter, and then Chinese search engine Baidu, briefly diverting visitors to those Web pages to a different page decorated with an Iranian flag, nationalist slogans and anti-U.S. and anti-Israel images.

"We are not sure if they are really Iranians," Mr. Raff said of the ICA, "But they are supporters of the Iranian regime."

He said his firm was trying to identify the geographical origin of the attacks, but such tracing is notoriously difficult in cyberspace, where hackers can launch attacks from computers they control half a world away from their own location.

"At the moment, there is no way of knowing who these people really are," said Jason Glassberg, of the computer firm Casaba Security.

"They could be Iranians," he told The Times, "It could just as easily be a 13-year-old in New Jersey."

Politically motivated cybervandalism like the ICA defacement of the Twitter and Baidu sites is relatively common, and usually no more than a nuisance. For example, Islamic hacker groups, many of them apparently based in Turkey, defaced Danish websites after a newspaper there published cartoons of the Prophet Muhammad in September 2005.

But ICA's most recent hack appears to be much more aggressive, said Mr. Raff. He said European newsblog site TechCrunch, and "hundreds" of other smaller sites that use WordPress had been compromised over the past two months. Visitors were surreptitiously redirected to a hacker-controlled website, where they were infected with a so-called Trojan downloader -- a kind of malicious software that allows hackers to take control of the user's computer.

The Trojan was placed on the visitors' computers by exploiting well-known vulnerabilities in several widely used software packages, including Adobe PDF, Java and Internet Explorer.

Seculert linked the ICA to the WordPress-based attacks through an e-mail address that was also referenced in the Twitter defacement attack. The firm's researchers found the Web page ICA was using to control its botnet, and noted that their Trojan software appeared to be infecting thousands of computers an hour.

Given that the vulnerabilities ICA is using are known and that anyone whose computer software was properly patched and up to date would be immune, Mr. Raff said it was "scary to see that people are still getting infected" at such a rate.

He estimated that millions of computers could be in the ICA botnet, but other analysts downplayed those figures.

"You can't really assume a constant rate of infection," said Steven Adair of the Shadowserver Foundation, a volunteer group of security professionals that tracks illicit activity on the Internet. He added that the estimate also might involve multiple counting of computers that had been infected more than once.

"I would say that estimate is likely on the high side," he said.

Botnets can be used to send spam e-mail or spread more malware, but they can also be used to conduct so-called denial-of-service attacks against websites. At the moment, Mr. Raff said, the ICA appeared to be selling access to the computers it had infected to other cybercrime gangs, who were loading their own malware onto them, effectively recruiting them to multiple other botnets, or equipping them to steal banking passwords or other personal data from their owners.

"They have moved into commercial cybercrime," said Mr. Raff of the ICA. "But we suspect that they will also use [their botnet] in the future for hacktivist attacks," perhaps in the service of Tehran.

Russian nationalist hacktivists were blamed for providing the foot soldiers for the cyberwar attacks on Estonia in April and May 2007. Those hackers used botnets to cripple Estonian government and banking websites.

Mr. Raff said the ICA attack had been reported to law enforcement in several countries and was under investigation but declined to comment further.

Over the summer, security researchers assessed that a computer worm called Stuxnet, which attacked special industrial-control systems, had been aimed at sabotaging an Iranian nuclear plant. Given the timing of the ICA attack, Mr. Raff said, "on the heels of the recent Stuxnet worm -- it appears reasonable to assume that the Iranian Cyber Army group has decided to move from simple defacement warnings to actual cybercrime activities."

4. Republican Aides Say Cybersecurity Bill Will Wait for Next Year

Tim Starks, CQ.com, 26 October 2010

Senior Republican aides said Tuesday it appears unlikely that the Senate will clear cybersecurity legislation in the upcoming lame-duck session, but they said the prospects for a similar measure will improve in 2011.

Speaking on a Heritage Foundation panel, Brandon Milhorn, the top GOP staff member for the Homeland Security and Governmental Affairs Committee, and Louis Tucker, the top Republican aide on the Intelligence Committee, outlined the difficulties of enacting a cybersecurity bill in the short term.

The Homeland Security and Governmental Affairs Committee has combined its cybersecurity bill (S 3480) with the Senate Commerce, Science and Transportation Committee bill (S 773), but hasn't resolved every issue, Milhorn said. Outstanding topics include what to do with a provision of the measure – sponsored by Homeland Security and Governmental Affairs Chairman Joseph I. Lieberman, I-Conn., top GOP member Susan Collins, R-Maine and Thomas R. Carper, D-Del. – that would provide liability protections to companies acting on demands from the executive branch during a cyber-emergency.

Senate Majority Leader Harry Reid, D-Nev., has brought together all the committees with cybersecurity jurisdiction to hammer out a bill, but Milhorn said the Commerce and Judiciary panels still need to resolve differences between their respective proposals for dealing with private-sector data breaches (S 3742, S 1490), including notifications to affected consumers.

Tucker said the crowded agenda for the remainder of 2010 could force cybersecurity to the back of the line. "There are only a few weeks left to accomplish an awful lot," he said. The two most senior Republicans on the Intelligence panel, Christopher S. Bond of Missouri and Orrin G. Hatch of Utah, are pushing their own cybersecurity bill.

Milhorn held out hope that Congress could act before 2011.

"I think we're in a position where we could take action now," he said. But he acknowledged that "a lot of things would have to come together in the context of the lame duck."

But the aides said that by 2011, Congress should be in a better position to act. How Congress proceeds will depend in part on who is in control of the House and Senate, Tucker said, and a major attack would probably increase the likelihood of a bill passing. Milhorn said that if Congress doesn't get bogged down in unrelated controversial issues, next year could offer a window for cybersecurity legislation.

"I think there's going to be an incredibly strong urge to get something done on this," he said. "By next year, something does get done."

Source: CQ Today Online News

© 2010 Congressional Quarterly Inc. All Rights Reserved.

[Back To Table Of Contents](#)

5. Cyber Threat to DHS Networks Continues to Grow

Rob Margetta, CQ.com, 26 October 2010

A cybersecurity official with Customs and Border Protection presented a dire view of the threat picture for federal computing systems Tuesday.

"It really is all bad," Alma Cole, the branch lead for the CBP Security Operations Center told an audience at the Institute for Defense and Government Advancement's 6th Annual Border Management Summit. "It's the Wild West."

Cole, who works with CBP in its role as steward for OneNet, a project intended to consolidate all Department of Homeland Security networks, said that federal data security workers used to be able to ensure a decent level of safety by getting users to avoid joining chat groups or making foolish downloads to their workstations. Now, he said, they are at risk when doing perfectly acceptable work.

"We have users that are infected every day . . . that are doing very legitimate things like Google searches," he said.

Worse, he said, is an explosion of malware proliferation in recent years, with new bugs developing at such a rate that at least half of them lack a profile that antivirus software could use to block them.

"There are so many new threats that are coming out that are not protected by antivirus, that it makes traditional antivirus almost useless," he said.

Government networks, in particular, are targeted by what's known in **cybersecurity** circles as "advanced persistent threats," Cole said. Those threats are characterized by the fact that they're launched by attackers with specific objectives, who engage in advance planning and don't mind making a long-term commitment to wait after gaining access to a system. Rather than using what Cole called "brute force," such attacks attempt to open a back door in a network, which can be present for weeks or even months before it's utilized.

Cole showed examples of one advanced attack technique called "spear-phishing," a refinement of the "phishing" e-mails that clog inboxes across the country. Rather than offering links to discount pharmaceuticals or other temptations, the more sophisticated attacks target their messages to their recipients, he said.

In one case, a CBP user received a message from an unfamiliar sender, but with a link to a file on a subject with which he was familiar. The file came with a virus attached, Cole said. Another example used a real **FBI** intelligence bulletin with one valid link to an **FBI** Web site, but another fake link that transmitted malicious coding. Such coding can allow attackers to record a user's key strokes, capture audio from a computer's built-in microphone or video from its camera, extract passwords or install programs.

"This is all very, very real," Cole said, comparing the level of concern to Cold War worries about listening devices. The problem has only become exacerbated as workers integrate technology into their daily lives, he said. Many now want to be able to access services such as social networking from the office, which can lead to security vulnerabilities.

Cole said addressing the threats requires abandoning some conventional concepts of **cybersecurity**, including the idea that users' computers can be sacrificed so long as sensitive networks remain protected. In reality, he said, attackers can exploit any vulnerability to move deeper into a system. Firewalls and other traditional security methods "are really failing us," he said.

Also lagging behind is the government's traditional way of gathering resources to address security problems. Cole said the establish method of soliciting, receiving bids, awarding a contract and waiting for deliverables simply can't keep up with evolving cyber threats.

"By the time you have the product in hand two years later . . . the threat has changed," he said.

DHS does have plans in place to combat the security issues, he said. Currently, the department is employing strategic monitoring to identify infected users and block off malicious software before it spreads. What the department is striving for is a way to create a search capability for all legitimate users' access to applications on federal networks, so it can audit user behavior and search for threats.

"That is an incredibly difficult challenge," Cole said.

DHS also continues to move forward with the Trusted Internet Connections initiative, a project intended to cut down the number of connections between its networks and the larger Internet, Cole said.

Source: **CQ Online News**

© 2010 Congressional Quarterly Inc. All Rights Reserved.

[Back To Table Of Contents](#)

UNCLASSIFIED

6. Republicans Probe Gitmo Transfers to Europe

Evan Perez, Wall Street Journal, 27 October 2010, Page A6

WASHINGTON — Republicans who have blocked the Obama administration from closing the Guantanamo Bay prison for terror suspects are now questioning its moves to transfer some detainees to Europe.

Republican staffers on the Senate Intelligence Committee recently traveled to Spain, Germany, France and other countries to dig for evidence of lax oversight of former detainees transferred there, according to people familiar with the matter.

The trip is an indicator of the next phase of the fight over the Guantanamo prison, a frequent flashpoint in debates over national security and the war against al Qaeda terrorists. President Barack Obama ordered it closed on his second day in office, but quickly retreated after opposition from Republicans and some Democratic lawmakers.

The transfer of detainees has been the administration's most successful strategy to reduce the Guantanamo population. It has resettled or moved 66 people, mostly to European countries.

In moving detainees abroad, the Obama administration is following in the footsteps of the Bush administration, which released hundreds of men from Guantanamo.

The prison now houses just over 170 detainees, including 24-year-old Canadian Omar Khadr, who pleaded guilty this week to charges including throwing a grenade that killed a U.S. soldier in Afghanistan. The U.S. said it would support Mr. Khadr's move to Canada after he serves another year at Guantanamo.

With Republicans expected to make major gains in Congress in midterm elections, the question is whether the transfers can continue at the same pace.

Republicans cite an estimate from the Pentagon that some 20% of the detainees released under President Bush have returned to the fight. They say Mr. Obama should abandon the release policy in light of that figure. The Obama administration suspended transfers of detainees to Yemen after the botched airline bombing on Christmas Day 2009 by a Nigerian man who had trained in Yemen.

Sen. **Christopher Bond** of Missouri, the top Republican on the Senate Intelligence Committee, said the administration should "start prioritizing the safety and security of the American people over the so-called rights of these terrorists."

Mr. Bond and Sen. Jeff Sessions of Alabama, the top Republican on the Judiciary Committee, wrote to Attorney General Eric Holder in August seeking documents related to the decisions to transfer detainees. Mr. Sessions cited what he called the "administration's politicized rush to shut down Gitmo and release dangerous inmates." The Republican staff trip to Europe in late summer to meet with European security officials was part of the effort to illustrate problems with the administration's strategy.

Staffers familiar with the trip declined to say whether the delegation uncovered any evidence of detainees being in touch with suspected al Qaeda affiliates. Without offering details, they said some countries' monitoring of detainees differed from what the administration has described.

A U.S. official involved in overseeing the Guantanamo transfers said U.S. security officials receive regular reports from countries hosting transferred detainees.

The reports include details of behavioral problems by some detainees, some of whom are experiencing culture shock, the official said. The official disputed the notion that detainees resettled are dangerous, saying none "has been confirmed or suspected of re-engaging" with terror groups.

A congressional staffer said the trip was "routine oversight. This is what Congress is chartered to do, to oversee executive branch programs."

At least one detainee transferred under the Obama administration has joined the Taliban in Afghanistan, according to U.S. **intelligence officials**. Abdul Hafiz, who also used the name Abdul Qawi, was repatriated to Afghanistan in December 2009, after spending more than six years in Guantanamo. He was allegedly implicated in the killing of a Red Cross aid worker.

One problem for those hoping to slow down Guantanamo releases is a Supreme Court ruling entitling detainees to challenge their confinement in court. Some detainees have won lower-court rulings ordering their release, although final decisions are awaiting appeal.

Copyright 2009 Dow Jones & Company, Inc. All Rights Reserved

[Back To Table Of Contents](#)

UNCLASSIFIED

7. Psychiatrist: Detainee is 'highly dangerous'

In the sentencing phase of Omar Khadr's teen terror case, a forensic psychiatrist called the Canadian devout and angry.
Carol Rosenberg, Miami Herald, 27 October 2010

GUANTANAMO BAY NAVY BASE, Cuba -- Confessed teen terrorist Omar Khadr is a dangerous threat to the West, a "rock star" who has "been marinating in a radical Islamic community" inside Guantánamo's showcase camp for cooperative captives, a forensic psychiatrist hired by the Pentagon told a military jury Tuesday. "He is devout. He is angry," Dr. Michael Welner said. "He identifies with his family, which has radical leanings. He is not remorseful and he is not westernized although he is very articulate and smooth." Welner's testimony was sure to rattle Khadr's native Canada.

The United States intends to send the Toronto-born Khadr, 24, back to Canada next year to serve out the remainder of an eight-year prison sentence as part of a plea bargain.

But the jury doesn't know it.

The judge, Col. Patrick Parrish, told them only that Khadr pleaded guilty to five war crimes on Monday, finally admitting that at age 15 he hurled the grenade that killed Sgt. 1st Class Christopher Speer, 28, of Albuquerque, N.M., trained with al Qaeda and planted anti-tank mines targeting U.S. forces.

Now, first the prosecution then the defense are calling witnesses.

The seven-officer jury will deliberate a sentence that Khadr would only serve if it undercuts the plea bargain -- something prosecutors clearly sought to avoid with Welner's testimony. "He's highly dangerous," Welner said. "He murdered. He has been part of al Qaeda. And we're still at war." In one of those curious twists of coexistence between captives and captor at Guantánamo, the Army judge interrupted the doctor's discourse on the dangers of radical Islam to give Khadr time for his afternoon prayers.

When it resumed, the psychiatrist expounded on Khadr's celebrity. His family had the "stardust" of proximity with the bin Ladens, he said. At Guantánamo, Khadr may be the youngest but his elders confer on him the honor of prayer leader. Welner argued that the Khadr case kept

the spotlight on the controversial prison camps set up in 2002. "He's drawn more attention to Cuba than Fidel," said Welner, who graduated from the University of Miami.

For the next couple of days, lawyers are calling victims, including Speer's widow, and mental health experts to talk about the damage Khadr did as a child and his prospects as an adult. "I look forward to proving to the panel and the world that Omar Khadr is a kind, compassionate, and decent young man who deserves a first chance at a meaningful life," said Lt. Col. Jon Jackson, Khadr's Pentagon appointed defense lawyer.

© 2010 Miami Herald Media Company. All Rights Reserved.

[Back To Table Of Contents](#)

UNCLASSIFIED

8. Candid Talks by Detainee Were Caught on U.S. Tapes

Benjamin Weiser, New York Times, 27 October 2010, Page A25

Ahmed Khalfan Ghailani, the former Guantánamo detainee now on trial in Federal District Court in Manhattan, has been interrogated repeatedly over the years: by the **Central Intelligence Agency**, by the Federal Bureau of Investigation and by the Defense Department.

And while there has been much focus on what he said during those sessions, the government has also been listening to him in another way.

At the military prison at Guantánamo Bay, Cuba, the government was recording candid conversations he had with at least one other detainee.

The contents of the recordings are classified, and they have not been mentioned to the jury in Mr. Ghailani's trial, which has entered its third week.

But the existence of the recordings, which have been briefly cited in public court documents, suggests that the government has had another source of intelligence about detainees and could someday face the issue of whether such statements could be useful in a civilian court.

Mr. Ghailani is the first former Guantánamo detainee to be moved into the civilian system for trial, and his case has raised significant legal issues that could recur if the government tries detainees like Khalid Shaikh Mohammed in federal court.

The judge, Lewis A. Kaplan, recently barred prosecutors from using a witness who was found out about through interrogation of Mr. Ghailani when he was in **C.I.A.** custody, a time when his lawyers say he was tortured.

These recordings appear to have been made under less coercive conditions. "The recordings at Guantánamo" revealed Mr. Ghailani to be in "a relaxed state, in which Mr. Ghailani was quite candid with the other detainee," a court-appointed psychiatrist wrote to the judge after reviewing transcripts of the recordings.

The psychiatrist's reference to the recordings appears in a court document in which certain sections are blackened out. Neither prosecutors nor defense lawyers would comment for this article.

The reference does not indicate whether Mr. Ghailani was overheard making incriminating statements. He has been charged with conspiring in Al Qaeda's 1998 bombings of two American Embassies in East Africa, which killed 224 people.

But the recordings show how conversations overheard while Mr. Ghailani was in military custody were used by a court to help determine that he was competent to stand trial in a civilian court.

Citing the recordings and other materials, the psychiatrist, Dr. Gregory B. Saathoff, found Mr. Ghailani was not suffering from any mental illness that would render him incompetent for trial. He also said Mr. Ghailani did not suffer from post-traumatic stress syndrome; a defense psychologist had concluded that he did, saying it stemmed from his treatment in **C.I.A.** custody.

Prosecutors told the judge last year after Mr. Ghailani appeared in federal court that they would not be introducing against him any statements he "may have made while he was in custody of other government agencies."

Last April, prosecutors said they would not use at trial any statements Mr. Ghailani had made "in response to interrogation" while in **C.I.A.** or military custody. It would seem that the overheard conversations were not the product of interrogations, although Mr. Ghailani's lawyers have argued throughout the case that any statements he made in his nearly five years of detention are tainted and inadmissible.

Jonathan Hafetz, a national security law expert at Seton Hall University, said Mr. Ghailani's case "shows the variety of different purposes for which recordings might be used" in civilian court. It is not known how many other detainees' conversations have been recorded in the same manner.

It is known, though, that much activity at Guantánamo has been under surveillance. The government said in 2008, for example, that guards used round-the-clock video recording to "ensure good order and discipline" at the facility. And a 2008 report by the Center for Policy and

Research at Seton Hall Law School, called "Captured on Tape," said all interrogations conducted at Guantánamo since 2002 had been videotaped.

Copyright 2010 The New York Times Company

[Back To Table Of Contents](#)

UNCLASSIFIED

9. Terror suspect held at CIA secret prison gets victim status in Polish probe

Adam Goldman and Vanessa Gera, Associated Press, LATimes.com, 27 October 2010

WARSAW, Poland (AP) — Polish officials investigating a now-shuttered secret CIA prison in this country have given a Saudi terror suspect victim's status, a legal advance in the detainee's effort to show he was mistreated by interrogators, the man's lawyer said Wednesday.

Legal experts said Poland's move to grant the status of victim to Abn al-Rahim al-Nashiri recognizes the validity of his claims even as U.S. courts have refused to allow cases involving rendition to move forward for national security reasons.

Al-Nashiri, a Saudi national accused in the 2000 bombing of the warship USS Cole warship in a Yemeni harbor, was apprehended by the U.S., taken to secret CIA prisons in Poland and Thailand and subjected to harsh treatment, according to former U.S. intelligence officials.

"While this is a significant step forward, it remains to be seen whether the Polish prosecutor will push forward seriously with the investigation," said Amrit Singh, a senior legal officer for the Open Society Justice Initiative.

Polish officials in power when the prison was in operation still deny its existence but al-Nashiri's victim status weakens their position - and it raises the prospect that some could eventually be charged with abuse of power.

Adam Bodnar, a lawyer and activist with the Helsinki Foundation for Human Rights in Warsaw, said that al-Nashiri's victim status will give his lawyers the right to participate in proceedings, a practical advantage. The move, he said, also indicates that prosecutors believe there is mounting evidence to support al-Nashiri's claims.

"Granting such a 'victim status' means that the prosecutor's office is to a great extent convinced of the argumentation that he was rendered and held illegally on the territory of Poland," Bodnar said. "So basically it's an indirect acceptance that the arguments and facts presented by the lawyers are probable. It doesn't mean they are true - but that on balance there is the probability."

According to a motion filed in Poland last month, al-Nashiri's lawyers have asked Polish prosecutors to call several former top CIA directors to testify as well as pilots of the various flights that ferried the suspects in and out of Poland.

Former U.S. intelligence officials have said the spy agency operated the site code-named "Quartz" in northern Poland from December 2002 to the fall of 2003. Human rights activists and lawyers for al-Nashiri say their client was tortured in Poland and denied a fair trial for nine years.

Imprisoned at Guantanamo, he's accused of masterminding the Oct. 2000 attack on the U.S. destroyer off the coast of Yemen that killed 17 American sailors.

Prosecutions of any Polish officials who allowed the site to operate on Polish soil would bring al-Nashiri a measure of justice in his case, activists and the detainee's lawyers say.

"I'm very satisfied with the prosecutor's decision to admit al-Nashiri to the investigation as a victim," Mikolaj Pietrzak, al-Nashiri's Polish lawyer said. "I expect the case to end with indictments against those responsible for the illegal detention and torturing of al-Nashiri."

He added: "It means there is a chance that the Polish investigation will actually serve to vindicate al-Nashiri's rights."

The CIA, saying the program is a thing of the past, is trying to focus on preventing future terrorist attacks.

Al-Nashiri's lawyers believe he hasn't been tried yet because he was subjected to waterboarding and other harsh interrogation techniques in Poland and Thailand, making any evidence obtained at the black sites legally problematic to introduce in a court of law.

The investigation in Warsaw was launched by the Polish government two years ago in reaction to massive pressure from the European Union and the Council of Europe, a human rights group. Both organizations have said that evidence points to the complicity of Poland as well as Romania in the clandestine U.S. program, and they have urged both ex-communist nations to clarify the matter.

Former U.S. intelligence officials have told the AP that Al-Nashiri was captured in Dubai in November 2002 and taken first to a secret CIA prison in Afghanistan known as the Salt Pit. After a brief stay, he was flown to a CIA prison in Thailand and then transported to Poland on Dec. 5, 2002, along with accused terrorist Abu Zubayda, the former officials said.

According to the former intelligence officials and an internal CIA special review of the program, al-Nashiri was subjected to harsh interrogation methods. They say that an agency officer named Albert revved a bitless power drill near the head of a naked and hooded al-

Nashiri while he was held in the Polish prison. The CIA officer also took an unloaded semiautomatic handgun to the cell where al-Nashiri was shackled and racked the weapon's ammunition chamber once or twice next to his head, according to the review.

The U.S. officials spoke about the prison and al-Nashiri's case on condition of anonymity because details of the secret program remain classified. The details of where the incidents took place and who was involved were first reported by the AP in September.

According to the former officials and flight records, al-Nashiri was moved from Poland to Rabat, Morocco, on June 6, 2003, and then moved repeatedly to and from CIA sites in Guantanamo, Rabat and Romania until he was finally returned to Guantanamo in September, 2006.

Al-Nashiri's case is in limbo as the White House decides whether to prosecute him in a U.S. military or a federal civilian court.

Copyright 2010 Associated Press. All rights reserved.

[Back To Table Of Contents](#)

UNCLASSIFIED

10. U.S. Military Sees Additional Document Leaks Ahead

Julian E. Barnes and Joe Lauria, Wall Street Journal, 27 October 2010, Page A24

WikiLeaks is poised to publish additional material taken from classified military computer networks, U.S. defense officials said Tuesday, even as the White House absorbed calls to investigate recent leaked accounts of apparent American complicity in the torture of Iraqis.

The fallout came after WikiLeaks' weekend release of nearly 400,000 U.S. military reports from the Iraqi war that document, among other things, thousands of previously unreported civilian deaths in Iraq and U.S. knowledge of torture of Iraqis by local security forces. The U.S. has confirmed the documents' authenticity.

Pentagon spokesman Col. David Lapan said Tuesday the military believes WikiLeaks has more documents the military says were stolen from its networks. The WikiLeaks site carries a link to a large encrypted document, marked "insurance," that users can download. The site hasn't released a decryption key that would allow it to be read. It is unclear whether the Pentagon has decoded the file.

"We don't know for certain what's in the insurance file. So we don't know exactly everything that WikiLeaks has," Col. Lapan said. "We believe we know some of what they have."

The Pentagon's belief of the file's likely contents stems from an investigation of Private First Class Bradley Manning, according to another defense official. PFC Manning, an Army intelligence analyst, was arrested in May and charged with giving WikiLeaks a video that shows an Apache helicopter firing on Iraqi civilians. This official said computers used by PFC Manning have led investigators to other material he downloaded and that they believe he may have passed to WikiLeaks.

PFC Manning is charged with giving WikiLeaks one diplomatic cable. Before he was arrested, he had bragged to a former hacker that he had access to several diplomatic cables. The site hasn't released large numbers of diplomatic documents.

Also Tuesday, Manfred Nowak, the United Nations' chief investigator into allegations of torture, said the U.S. should probe revelations that it knowingly turned over suspects to be tortured by local authorities during the U.S. war in Iraq. He said the U.S. should appoint a special prosecutor, or an independent panel that could include international experts, to investigate the U.S. transfer of detainees for torture to Iraq and other countries. He named Morocco, Syria and Egypt.

Mr. Nowak said the leaked documents that outline U.S. prisoner handovers "confirm what we knew and heard" about the "brutality and torture systematically practiced by Iraqi security forces and irregular militias." He added: "It shows very clearly that the Bush and Obama administrations knew, and know, that when they are handing over detainees under U.S. custody to Iraqi security forces that there is a serious risk of them being subjected to torture."

Mr. Nowak said this marked a violation of the U.N.'s Convention Against Torture, which the U.S. Senate has ratified.

U.S. State Dept. spokesman P.J. Crowley said, "We have an agreement with Iraq where we have turned over responsibilities to Iraq as a sovereign government. These are more appropriate questions to direct to the sovereign government of Iraq, not to the United States."

Mr. Nowak also said a "full" U.S. investigation should also look into torture practiced directly by officials of the U.S. military, the Central Intelligence Agency and private security companies in Iraq, Afghanistan or the U.S.-run prison at Cuba's Guantanamo Bay. "The Senate intelligence committee has done certain investigations, but they are not in the public domain and they are not sufficient whatsoever," Mr. Nowak told a U.N. press conference.

He said the Bush and Obama administrations had not allowed him to visit U.S.-run detention centers in Afghanistan or Iraq, or to privately interview detainees in Guantanamo.

The U.S. mission to the U.N. did not comment on this aspect of Mr. Nowak's plea, referring only to the remarks made by Mr. Crowley on handing prisoners over to Iraq.

Mr. Nowak is among some three dozen "special rapporteurs"—unpaid experts the UN appoints to investigate human-rights violations but who are considered outside the UN system. These officials' power is limited: They must be invited by governments to investigate and they have no prosecutorial power.

Mr. Nowak, an Austrian academic, is leaving his post on Friday after serving the maximum term of six years.

Copyright 2009 Dow Jones & Company, Inc. All Rights Reserved

[Back To Table Of Contents](#)

UNCLASSIFIED

11. U.S.: Enemies Searching WikiLeaks Iraq Papers

Lara Jakes, Associated Press, Time.com, 26 October 2010

(BAGHDAD) -- U.S. enemies already are combing through data released last week in a trove of Iraq war documents for ways to harm the American military, the Pentagon's No. 2 official said Tuesday.

U.S. Deputy Defense Secretary William J. Lynn called the documents "stolen material" and said they give adversaries key insight on how the U.S. military operates. He did not say which groups, or how the Pentagon knew they were researching the documents.

"There are groups out there that have said they are indeed mining this data to turn around and use against us," Lynn told a small group of reporters during a brief visit to Baghdad. "We think this is problematic."

The Pentagon furiously opposed the documents' release Saturday by the whistle-blower WikiLeaks website. Lynn's remarks came a day after WikiLeaks founder Julian Assange told CNN that the nearly 400,000 papers did not put troops at risk because the names of any soldiers or Iraqi civilians have been redacted.

The U.S. has said that the WikiLeaks release of secret Afghan and Iraq war documents threatens national security.

WikiLeaks posted about 77,000 Afghanistan war logs on its site in July, and the Pentagon concluded that no U.S. intelligence sources or practices were compromised by the posting. A few weeks later, Defense Secretary **Robert Gates** said he was not yet aware of any Afghan people who were killed as the result of the leak, "but I put emphasis on the word 'yet.'"

Lynn said the leaked information would not change the way the estimated 50,000 U.S. troops in Iraq operate. But he said he is mulling ways to keep more documents from leaking in the future, such as having computer systems monitor for irregular data searches.

"It does seem like commonsense, and I don't think we're doing enough of it, frankly," Lynn said.

In Washington, Pentagon spokesman Marine Col. David Lapan said WikiLeaks may have even more classified material than U.S. officials previously believed. He declined to characterize it, but WikiLeaks already has posted half a million secret Iraq and Afghanistan war files since July.

The group is also believed to have another 15,000 Afghan war field reports, 260,000 diplomatic cables and U.S. video of casualties in Afghanistan.

At the center of the WikiLeaks controversy is a former intelligence analyst, Army Pfc. Bradley Manning, who is under suspicion of having provided the classified military documents to the whistle-blower website. Manning was stationed in Iraq when he was arrested by U.S. authorities last May. He is charged with multiple counts of mishandling classified data and putting national security at risk.

Meanwhile, the United Nations' top human rights official called the U.S. and Iraq to investigate allegations of detainee abuse contained in the newest WikiLeaks' war logs. The document cache contained reports of severe abuse by Iraqi forces, and showed that U.S. troops did not intervene to halt the violence in many cases.

U.N. High Commissioner for Human Rights Navi Pillay said the information adds to "concerns that serious breaches of international human rights law have occurred in Iraq."

Pillay said that the U.S. and Iraq should prosecute anyone believed responsible for torture, unlawful killings and other abuses.

The documents show that U.S. forces turned detainees over to Iraqi forces even after signs of abuse.

Anne Flaherty in Washington contributed to this report.

Copyright © 2010 Time Inc. All rights reserved.

[Back To Table Of Contents](#)

12. WikiLeaks has more US war files, Pentagon says

* *WikiLeaks threatens to release more Afghan war documents*
 * *Group already has released 500,000 US Iraq, Afghan files*

Phil Stewart, Reuters.com, 26 October 2010

WASHINGTON, Oct 26 (Reuters) - WikiLeaks, which already has made public nearly 500,000 classified U.S. files on the wars in Iraq and Afghanistan, has more U.S. documents for possible release than it has stated, the Pentagon said on Tuesday.

The massive WikiLeaks disclosures of leaked documents have been the largest in U.S. military history, and Pentagon officials are saying that more files may follow.

The whistle-blowing organization has publicly acknowledged it has some 15,000 more documents on the war in Afghanistan that it has threatened to release, along with an Afghanistan video file, the Pentagon noted.

"Those are things they've talked about publicly. And we have reason to believe they have other documents as well," Colonel Dave Lapan, a Pentagon spokesman, told reporters.

Asked whether the Pentagon had independent knowledge of what WikiLeaks had in its possession, he said: "We do," without elaborating.

The U.S. investigation into the source of the leaks has focused on Bradley Manning, a former U.S. Army intelligence analyst in Iraq. Manning is under arrest, charged with leaking a classified video showing a 2007 helicopter attack that killed a dozen people in Iraq, including two Reuters journalists.

No one has yet been charged with leaking any of the more than 70,000 files on the Afghanistan war that WikiLeaks released in July or the nearly 400,000 Iraq war files disclosed last Friday.

Manning's attorney did not return phone calls. The Pentagon has refused to discuss the investigation.

WikiLeaks founder Julian Assange has said the U.S. investigation is also looking into WikiLeaks itself.

Lapan said the Pentagon believes it knows which documents WikiLeaks has in its possession, including a large, encrypted file on its website entitled "insurance," which has not been released to the public.

"We believe we know some of what they have," Lapan said.

"We don't know for certain. For example, we don't know for certain what's in the 'insurance' file. So we don't know exactly everything that WikiLeaks has."

Earlier on Tuesday in Baghdad, a top Pentagon official said the U.S. Defense Department was considering controls like those that credit card firms use to detect odd behavior to prevent leaks of sensitive information.

"Rather than preventing people from having access to the data, could we do things like credit card companies do, which is to look for anomalous behavior," Deputy Defense Secretary William Lynn told reporters during a brief visit to Iraq.

"If someone is doing something that doesn't seem appropriate for where they are, downloading 100,000 documents when they are out in some obscure corner of the country, why are they doing that? You go out and ask them," Lynn said.

(Additional reporting by Michael Christie in Baghdad; Editing by Will Dunham)

© Thomson Reuters 2010. All rights reserved.

[Back To Table Of Contents](#)

13. In Information Age, Leaks Are Here To Stay

Tom Gjelten, NPR.org, 26 October 2010

Given the problems hanging over WikiLeaks founder Julian Assange – his fundraising difficulties, the threat of prosecutions in the U.S. for espionage and in Sweden for rape, and the resignation of key staff -- the survival of his whistle-blower organization cannot be assured.

Leaks, however, are here to stay.

The disclosure of secret intelligence files is in many ways a phenomenon of the information age, and national security officials in the U.S. and other countries need to prepare for the consequences, WikiLeaks or no WikiLeaks.

"Almost all sensitive information is in electronic form," says Steven Aftergood, director of the Government Secrecy Project at the Federation of American Scientists. "So it is possible to transfer it and transport it anywhere. In the old days, it was necessary to lug around large volumes of hard-copy materials."

Now they can be e-mailed. Plus, officials now believe in the value of sharing intelligence, both sideways between government agencies, and top to down --from military commanders to frontline soldiers.

"We want those soldiers in a forward operating base to have all the information they possibly can have that impacts on their own security," said Defense Secretary **Robert Gates** this summer, while discussing the first WikiLeaks disclosures.

These changes in the way intelligence is collected, used and shared means the risk of it being leaked is inevitably greater.

Leaks these days also have a wider and more immediate impact. Thanks to the Internet, secrets spread almost instantaneously around the globe. When word of the Iran-Contra scandal broke more than 20 years ago in Lebanon, it took weeks for the news to spread to the U.S. That would not be the case today.

Why Disclose Secrets?

The key question is what this all means for relations between the government and the public, and whose interests are served.

"This disclosure is about the truth," Assange said last week, quoting Phillip Knightley's observation that truth is the first casualty of war.

"In our release of these documents about the Iraq war," Assange said, "we hope to correct some of that attack on the truth."

The argument for divulging government secrets is that it keeps governments accountable for their actions. But indiscriminate leaks can violate privacy, jeopardize national security and produce little of value, even to government whistle-blowers.

"The fascination with classified documents tends to wear off rather quickly," Aftergood says. "They are not intrinsically interesting, and -- contrary to what WikiLeaks proclaims -- they are not always the truth.

"There's no more truth to be found in classified records than there is to be found in unclassified records."

'An Adult Conversation'

Indeed, many of the files released by WikiLeaks were raw, uncorroborated intelligence reports, describing events before all the facts were known.

"The problem is not whether the public should have more access. They will," says Philip Zelikow, who served as executive director of the 9/11 Commission and at the National Security Council under George W. Bush. "The problem is that the public gets some of the information but it only gets fragments of the information."

What does it all add up to? Government leaders must now assume that some of the intelligence reports on which they base their decisions will eventually become public. Knowing that, they will need to make the case for their policies more carefully.

Retired Air Force Gen. Michael Hayden, a former **CIA** director, says he agrees with those who argue that the government keeps more secrets than it needs to. But declassification, he says, should proceed carefully.

"There are some things that are simply legitimately secret," he says. "We need an adult conversation, kind of a social contract, between American society and America's espionage agencies as to how much should you know."

One thing is clear: Given the amount of intelligence now being collected, the extent and ways it is shared, and the public's demand to know, the WikiLeaks story is likely to be repeated many times over. **CIA** directors, military commanders and government officials need to prepare themselves.

Copyright 2010 NPR

[Back To Table Of Contents](#)

UNCLASSIFIED

14. Taliban unscathed by U.S. strikes

Greg Miller, Washington Post, 27 October 2010, Page A1

An intense military campaign aimed at crippling the Taliban has so far failed to inflict more than fleeting setbacks on the insurgency or put meaningful pressure on its leaders to seek peace, according to U.S. military and **intelligence officials** citing the latest assessments of the war in Afghanistan.

Escalated airstrikes and special operations raids have disrupted Taliban movements and damaged local cells. But officials said that insurgents have been adept at absorbing the blows and that they appear confident that they can outlast an American troop buildup set to subside beginning next July.

"The insurgency seems to be maintaining its resilience," said a senior Defense Department official involved in assessments of the war. Taliban elements have consistently shown an ability to "reestablish and rejuvenate," often within days of routed by U.S. forces, the official said, adding that if there is a sign that momentum has shifted, "I don't see it."

One of the military objectives in targeting mid-level commanders is to compel the Taliban to pursue peace talks with the Afghan government, a nascent effort that NATO officials have helped to facilitate.

The blunt intelligence assessments are consistent across the main spy agencies responsible for analyzing the conflict, including the CIA and the Defense Intelligence Agency, and come at a critical juncture. Officials spoke on the condition of anonymity because they are not authorized to discuss the matter publicly.

The Obama administration's plan to conduct a strategic review of the war in December has touched off maneuvering between U.S. military leaders seeking support for extending the American troop buildup and skeptics looking for arguments to wind down the nation's role.

Gen. David H. Petraeus, the top U.S. commander in Afghanistan, has touted the success of recent operations and indicated that the military thinks it will be able to show meaningful progress by the December review. He said last week that progress is occurring "more rapidly than was anticipated" but acknowledged that major obstacles remain.

U.S. intelligence officials present a similar, but inverted, view - noting tactical successes but warning that well into a major escalation of the conflict, there is little indication that the direction of the war has changed.

Among the troubling findings is that Taliban commanders who are captured or killed are often replaced in a matter of days. Insurgent groups that have ceded territory in Kandahar and elsewhere seem content to melt away temporarily, leaving behind operatives to carry out assassinations or to intimidate villagers while waiting for an opportunity to return.

U.S. officials said Taliban operatives have adopted a refrain that reflects their focus on President Obama's intent to start withdrawing troops in the middle of next year. Attributing the words to Taliban leader Mohammad Omar, officials said, operatives tell one another, "The end is near."

Obama's decision to order an additional 30,000 troops to Afghanistan divided some of his senior advisers. While no major change in strategy is expected in December, critics could use the latest assessments to argue that the continued investment of American resources and lives is misguided, particularly when the main impediment to progress that analysts cite is beyond American control.

U.S. officials said the two main branches of the insurgency - the Taliban and the Haqqani network - have been able to withstand the American military onslaught largely because they have access to safe havens in Pakistan.

A crackdown by Pakistan's military on those sanctuaries probably would have a greater impact on the war than any option available to Petraeus, officials said. But given the Pakistani government's long-standing connections to the Haqqani network and the Taliban, a move by Islamabad against those groups is considered unlikely, at least by the administration's timetable.

The United States has sought to compensate by ramping up Forces raids and military air patrols on the Afghan side of the border, and by sharply increasing the number of CIA drone strikes in Pakistan.

Over the past two months, the spy service has nearly doubled the pace of its drone campaign, killing dozens of militants in territory controlled by the Haqqani network and thought to be a haven for al-Qaeda leaders, including Osama bin Laden.

Omar and other leaders of the Afghan Taliban are thought to be based primarily in Quetta, a sprawling Pakistani city that the Islamabad government does not allow CIA drones to patrol.

The joint CIA-military efforts have scrambled insurgent networks, causing senior operatives to move more frequently and become more preoccupied with security. Still, U.S. officials said the impact on the Taliban's highest ranks has been limited.

"For senior leadership, not much has changed," the defense official said. "At most we are seeing lines of support disrupted, but it's temporary. They're still setting strategic guidance" for operations against coalition forces in Afghanistan.

That guidance has shifted in recent weeks, officials said. The arrival of thousands of additional U.S. and coalition troops in the Taliban's stronghold around Kandahar has prompted insurgents to back away and embrace smaller-scale strikes.

"The enemy's tactics have shifted - to include intimidation and assassination," a U.S. intelligence official said.

The defense official said that as many as 100 Afghan government representatives in and around Kandahar are being targeted for assassination by the Taliban, according to U.S. military intelligence estimates.

U.S. officials stressed that the recent assessments are a snapshot of the nine-year-old war and that Petraeus's offensive has been underway for only a few months.

During that period, U.S. military officials said, the tempo of American operations has increased four- or fivefold. Last month, officials

disclosed that 235 insurgent leaders had been captured or killed in the preceding 90 days. At the same time, Air Force statistics showed that U.S. warplanes and drones had dropped or fired 700 weapons on Afghan targets in September, compared with 257 in the same month the previous year.

U.S. officials said they have seen isolated indications of slumping morale among some Taliban units, including a reluctance among some mid-level commanders to replace superiors who were captured or killed, apparently out of fear that they might meet the same fate.

But those examples have been offset by other instances in which Taliban succession is almost seamless. In northwestern Bagdhis province, for example, U.S. special operations forces thought they had delivered devastating blows to Taliban guerrillas, killing the group's local leader, Mullah Ismail, as well as his apparent heir, only to watch yet another "shadow governor" take the job.

The Taliban has dispatched lieutenants to engage in discussions with the government of Afghan President Hamid Karzai. But U.S. intelligence officials said the Taliban envoys seem to be participating mainly out of curiosity, convinced that they are in a position to prevail.

"If there are elements that wish to reconcile . . . that ought to be obviously explored," CIA Director Leon E. Panetta recently told reporters. "But I still have not seen anything that indicates that at this point a serious effort is being made to reconcile."

© 2010 The Washington Post Company

[Back To Table Of Contents](#)

UNCLASSIFIED

15. Afghan aid spent with little local input, audit finds

Karen DeYoung, Washington Post, 27 October 2010, Page A14

U.S. and other international development programs in a key Afghan province are "incoherent" and lack mechanisms to avoid wasteful overlap or to monitor their success, according to a new report by government auditors.

More than \$100 million in U.S. aid to Nangahar province, an area in eastern Afghanistan often cited as a model for success elsewhere in the country, was spent in fiscal 2010 with little or no input from local officials, according to the audit by the congressionally mandated Special Investigator General for Afghanistan Reconstruction, or SIGAR.

A separate SIGAR report released Tuesday warned of insufficient training of U.S. Foreign Service officers and other government civilians working throughout Afghanistan as part of the Obama administration's "civilian surge." The number of civilians has tripled since early last year and is expected to reach 1,500 by January 2012, rivaling the U.S. Embassy in Iraq as the world's largest.

The report said the State Department has done a good job of providing housing and other support for the rapidly growing workforce. But it faulted the effort to integrate civilian and military forces, saying that goals were often undercut by reliance on "ad hoc arrangements and individual personalities" rather than any agreed standards.

SIGAR was modeled after an investigative body set up to audit the multi-billion-dollar U.S. reconstruction program in Iraq, where vast corruption and waste was uncovered. Some in Congress have cited SIGAR for not being aggressive enough in examining massive U.S. expenditures in Afghanistan, estimated at about \$100 billion in combined military and civilian activities this year.

Spending for Afghanistan from 2001 to the end of fiscal 2010 totaled about \$336 billion, about \$60 billion of it for non-military "reconstruction" projects. The total is less than half the cumulative expenditures in Iraq, beginning in 2003, although annual Afghanistan funding exceeded Iraq for the first time this year.

'Increasingly concerned'

In its July quarterly report to Congress, SIGAR said it was "increasingly concerned" that the reconstruction effort in Afghanistan was impeded by lack of accountability and oversight, inadequate metrics and attention paid to sustainability of projects, and insufficient Afghan institution-building.

All of those concerns arose in the Nangahar audit. Afghanistan's second-largest revenue-producing province and the most densely populated, its capital city of Jalalabad sits astride the main highway between Kabul and Peshawar. Although security is said to have deteriorated over the past year, it is considered a relatively stable part of the country.

The province spends 85 percent of its \$60 million operating budget on wages for government employees and about 4 percent on development projects. "The U.S. government and other donors fund most of the development in Nangahar," the SIGAR report said, "but do not track funds or coordinate provincial funding with other donors."

Major donors, including the United States and the United Nations, "do not routinely collect or disseminate detailed data," or separate what they are doing in Nangahar from countrywide expenditures. "As a result," the report said, "U.S. officials . . . do not have the information necessary to effectively monitor and evaluate USAID programs."

Information on projects funded by the Commander's Emergency Response Program, through which the U.S. military dispensed \$58 million in development aid to Nangahar this year, and USAID, which spent about \$42 million, is not reported to the Afghan government, it said.

The report said that the province lacks an overall development plan and that local officials have virtually no control over decisions on where donor money is spent. It is also critical of the government in Kabul, which it said controls all funding, appointments and contracting in Nangahar without local input. U.S. policy in Afghanistan calls for empowering government levels below Kabul, but "provincial officials are effectively disenfranchised" by the current system.

Despite U.S. rules requiring that projects be sustainable, the report said, "Nangahar's provincial officials cannot manage or maintain what they cannot see, and most of the externally funded U.S. and international development activities we identified . . . are implemented without the input or visibility of provincial officials." Nangahar officials, it said, "are severely limited in their ability to sustain U.S.-funded development projects."

Lack of planning by the U.S. and Afghan governments, it said, "has resulted in an incoherent approach to development because accomplishments cannot be measured against needs identified in a plan, and ultimately impeded capacity development within the provincial government."

'Systemic obstacles'

In a response to the report, the U.S. Embassy in Kabul said that it recognized "systemic obstacles" to local management of development and the provincial budget but that "this is a matter of Afghan law" giving such powers to the central government. "All the governor and other provincial officials have is the power of persuasion," the embassy said of the provincial relationship with the national government.

In its "civilian surge" report, SIGAR said civilians working in the field "at all levels" raised concerns about the increase, "including the effectiveness of training; level of agency guidance . . . [and] models for civilian-military integration," as well as the "long-term sustainability" of the surge.

In the rush to fill personnel quotas, the report said, civilians new to the U.S. government, while technically qualified, "lack complete understanding of their agencies' missions and operating procedures." Some officials interviewed by SIGAR said that they were not told their assignments or deployment locations before arriving in Kabul and that their job descriptions were vague.

The report also said some civilian officials felt their knowledge of policy and procedures was inadequate compared with the military. "When civilians cannot provide quick responses to their military counterparts," it said, "they are viewed as being ineffective."

© 2010 The Washington Post Company

[Back To Table Of Contents](#)

UNCLASSIFIED

16. Afghan security problem: Poorly built police stations

Marisa Taylor and Warren P. Strobel, McClatchyDC.com, 26 October 2010

WASHINGTON — U.S. government auditors who've been examining Afghan construction projects have found serious problems with a crucial part of the Obama administration's plans to bolster the country's security forces so American troops can begin to leave next July.

McClatchy has obtained an upcoming report by the special inspector general for Afghanistan reconstruction that says six police stations in a dangerous stretch of southern Afghanistan were so poorly constructed by the Afghan contractor, Basirat Construction Firm, that they can't be occupied.

The SIGAR report, which is about to be released, concludes that conditions at the stations are so hazardous that "inadequate concrete and foundation work calls into question the structural integrity of the buildings and raises the risk of total building collapse in the event of a significant earthquake."

The U.S. Army Corps of Engineers nonetheless passed up chances to penalize Basirat and paid it almost \$5 million of the \$5.5 million contract price, according to the report.

SIGAR concludes that the company would have to make at least \$1 million in repairs before the buildings could be occupied. However, Basirat "has little incentive" to address the problems because it's been paid and it's unlikely to win any more contracts from the U.S. government, the report says.

The Army Corps of Engineers has embarked on a multi-billion-dollar construction program to house the Afghan National Army and National Police, which are the backbone of President Barack Obama's plans to start withdrawing American troops from the country next July.

The six police stations were designated for districts in tense Kandahar and Helmand provinces in southern Afghanistan, where U.S. troops are battling the Taliban-led Afghan insurgency.

The stations represent a pattern that current and former U.S. officials said had been repeated across Afghanistan: failures resulting from an overextended Afghan contractor working in a remote area where security has worsened because of a growing insurgency and with insufficient U.S. Army oversight.

Making matters worse, some Afghan firms are loaded down with "contract after contract" in the rush to build, even though they're not equipped to handle major projects, said John Brummet, a SIGAR assistant inspector general for audits.

In the case of the Basirat contract, the Army Corps of Engineers subcontracted oversight to local Afghans.

When auditors later arrived at the sites, they found electrical wires strung through windows, cracks in walls, gas lines hanging in the open, windows installed at a tilt and shoddy roofing.

At one site, in Helmand province's Nad Ali district, an Afghan police unit "forcibly occupied" the uncompleted structure and intentionally destroyed half the roof, a development that seems to bode ill for long-term maintenance of police headquarters across Afghanistan, even when they're properly constructed.

The report also documents a case in which local quality monitors hired by the Corps of Engineers submitted photographs that purported to document construction progress. However, the photographs' digital time stamps had been altered or erased.

The Army Corps of Engineers agreed with SIGAR's assessment of the construction problems, but said the lack of security in the area prevented it from monitoring the projects.

SIGAR, however, countered that security concerns don't explain why the corps "failed to retain adequate project funds as hedge against poor contractor performance and authorized payments without sufficient justification."

Yamae er Shadi, a Basirat program manager, acknowledged in a telephone interview that the company had won the contracts "at a very low price" and now "we have a shortage of money" to complete the work. He added that he's job hunting because he doesn't expect the company to pay him in the future.

Kenneth Moorefield, a Pentagon assistant inspector general, told Congress late last year that, "There are few Afghan companies with the requisite experience to effectively undertake and complete projects at the required standards."

"While many Afghans gladly accept the offer of employment, most are not qualified to contribute more than manual labor," he said.

In some cases, even the laborers may not be up to the job.

Falls Church, Va.-based DynCorp International LLC had to train its construction workers to hammer nails and pour concrete at the site of a project to build an Afghan army garrison, SIGAR found in an earlier audit.

Basirat's problems didn't begin or end with the police station contract.

The State Department suspended the company in August from new U.S. government contracts because of allegations of corruption related to its work on a \$26.5 million renovation of Pol-i-Charki prison outside Kabul. Basirat was awarded a contract to oversee the renovation in July 2009, despite the Army Corps of Engineers having removed it months earlier from two other failed police station projects.

The department is investigating allegations, which Basirat has denied, that it improperly colluded with another Afghan-based firm, Al Watan Construction Co., to help it win some of the prison renovation work. Al Watan has been suspended, as well.

Basirat also allegedly bribed a former U.S. official who'd overseen the prison project to help it prepare an appeal when it was kicked off yet another contract, according to Obaidur Rahman, the company's president.

In an e-mail response to questions, Rahman denied any impropriety. "I hope this problem will be resolved soon and I already apologized for not being aware of an 'ethics rule' violation to be applied when working with U.S. government projects," he wrote.

Rahman said that of the six police stations in Helmand and Kandahar, two had been completed and delivered, the Army Corps of Engineers was giving a final review to a third, a fourth was almost completed and the two others, in Kandahar, had encountered trouble with a subcontractor.

SIGAR is under pressure to demonstrate its ability to root out fraud and waste in Afghanistan after four senators recently wrote to Obama demanding the resignation of the agency's head, Arnold Fields, a retired Marine Corps major general.

The Justice Department reviewed the agency recently and decided not to revoke its law enforcement authority.

SIGAR released two reports Tuesday. One warned that massive foreign assistance in Afghanistan's eastern Nangarhar province, including an estimated \$100 million U.S. investment in fiscal year 2009, is at risk of being wasted because of haphazard coordination and the province's inability to absorb the aid.

The other report found confusion among U.S. civilians assigned to Afghanistan about their duties and whom they report to. The Obama administration has launched a civilian "surge" as part of its counterinsurgency strategy, with civilian personnel increasing from 320 to 1,500 by January 2012.

McClatchy Newspapers 2010

[Back To Table Of Contents](#)

17. Russia could play big role in Afghanistan after talks with Nato

Deborah Haynes, The Times, UK, 27 October 2010

The Russian military may play a new role in Afghanistan under plans being drawn up between Nato and Moscow -- more than two decades after Soviet forces were forced into a bloody retreat from the country.

Among a range of proposals under consideration is the possibility of Russia lending military helicopters to the Afghan Army, training Afghan pilots in Russia and enabling more Nato convoys -- including those with "lethal" cargo -- to pass across its territory. The plan could also extend to Russia training Afghan security forces outside the country in counternarcotics techniques.

Anders Fogh Rasmussen, the Secretary-General of Nato, said he hoped that details of the deal would be agreed at a landmark summit between Nato and Russia in Lisbon next month.

The meeting, to be attended by President Medvedev of Russia, will take place on November 20 at the same time as an annual summit of the heads of state of Nato, also in the Portuguese capital.

"I think there is potential for an expanded co-operation between Nato and Russia as regards Afghanistan," Mr Rasmussen said on Monday. "Russia has a long-term interest in stabilising the situation in Afghanistan because Russia's security is also affected by what is going on in Afghanistan, not to speak of the risk of destabilisation spreading from Afghanistan to Central Asia and farther."

The idea of Moscow taking a more active role will be hugely emotive in Afghanistan, where more than one million civilians lost their lives after the Soviet invasion in 1979. Nato officials appeared unconcerned at the potential psychological impact, noting that Russian-manufactured helicopters were already in use over Afghan soil.

Mr Rasmussen said that he raised the prospect of Russia providing the Afghan Army with helicopters at a meeting in Moscow in December. The concept is also being discussed between the US and Russia. "I would not exclude that we could facilitate that process within the Nato-Russia Council," Mr Rasmussen said. As well as aircraft, Russia could agree to let convoys of Nato weapons and ammunition cross its territory. Moscow already allows a limited number of largely non-lethal supplies to use its roads to gain access to Afghanistan.

Nato hopes that the Russian authorities will allow a larger number of convoys carrying a wider range of equipment. This would offer an alternative route for Nato from Pakistan, where the alliance's convoys come under regular attack from the Taliban.

The Nato-Russia summit could also lead to Moscow being invited to cooperate with the alliance on the controversial issue of missile defence.

"The summit will represent a new start in the relationship between Nato and Russia," Mr Rasmussen said. "Co-operation on missile defence will provide us with a very strong framework for developing a true EuroAtlantic security architecture."

Nato members are due to vote on whether to go ahead with a missile defence shield -- something that is widely expected, despite Turkey's disquiet -- at their annual summit on November 19 and 20. The shield, which would be largely funded and built by the US, is a scaled-back version of a plan advocated by the Bush Administration that drew strong objections from Russia. A warming of ties between the US and Russia after the arrival of President Obama at the White House, and a subsequent decision to "reset" relations, is seen as one of the main triggers for the closer Nato-Russia overtures.

Away from Russia, the alliance hopes to use its summit to agree a timeline for the transition of security across Afghanistan to Afghan forces by the end of 2014. It will also announce a long-term partnership between the alliance and Kabul that will come into force from 2015, signalling Nato's intention to remain in a supporting role with a heavily reduced presence.

"We will stay in Afghanistan as long as it takes to finish our job," the Secretary-General said. "Our clear goal is to hand over responsibility to the Afghans themselves. The Afghans should become masters in their own house and this process will start next year."

© Times Newspapers Ltd 2010

[Back To Table Of Contents](#)

UNCLASSIFIED

18. U.S. Tries Restart of Talks With Iran

Jay Solomon, Wall Street Journal, 27 October 2010, Page A1

WASHINGTON -- The Obama administration is pushing to revive a failed deal for Iran to send some of its nuclear stockpile overseas in exchange for assistance with peaceful nuclear technology, according to senior U.S. officials. The aim is to try to reduce Tehran's ability to quickly produce an atomic weapon.

Washington and other Western capitals are hoping Tehran will return to the negotiating table because they believe a fresh round of international economic sanctions against Iran--put in place after the previous fuel-swap deal fell apart last year--has begun to bite hard.

The U.S. is accelerating its efforts to present Iran with a new offer as part of broader talks on Iran's nuclear program planned for Vienna next month, according to three officials briefed on the diplomacy. Such a meeting would mark the first direct negotiation between U.S. and Iranian officials on the nuclear issue in more than a year.

On Tuesday, Tehran began loading Russian-supplied fuel rods into the core of its Bushehr nuclear plant. Iranian officials said they hoped the Bushehr plant, which the U.S. had lobbied Russia to delay, could begin producing power in two to three months. Tehran continues to maintain its nuclear intentions are peaceful, and Iranian President Mahmoud Ahmadinejad has remained publicly defiant toward the international community about Iran's program.

U.S. officials have been talking with allies about ways to expand the original fuel-swap deal to remove more of the stockpile, because Iran has been enriching more uranium since the previous talks broke down. Instead of 1,200 kilograms discussed then, Iran would need to agree to release or secure at least 50% more, or 1,800 kilograms, to stay below bomb-making levels, according to nuclear experts.

One idea the U.S. raised would send some of the stockpile overseas for eventual use in the Bushehr plant. But France rejected that idea because it risked legitimizing Iran's right to produce nuclear fuel, which the United Nations Security Council has opposed, spurring the sanctions. "We have to keep a focus on whether we're going to increase or diminish the pressure on Iran," said a European official briefed on the discussions.

Since the sanctions took effect, scores of international corporations and banks have severed their business ties to Iran, and Iranian businesses have said they've faced shortages of fuel and foreign exchange. Still, Western diplomats don't know what reception Tehran would give a new fuel-swap plan. During the most recent U.N. General Assembly in New York in September, U.S. officials indicated they thought Mr. Ahmadinejad was open to pursuing friendlier contact with the West, only to be disappointed when he gave a vitriolic anti-U.S. speech.

The original fuel-swap deal sought to ship more than half of Iran's low-enriched uranium stockpile to other countries in exchange for nuclear fuel usable in developing medical applications, but not enriched enough to make a nuclear bomb. Washington and its allies believe that if Iran's nuclear program is peaceful, it should be willing to have the fuel for civilian uses provided from overseas, reducing the potential for military diversion.

Talks on a new proposal among the U.S. and the five permanent U.N. Security Council members plus Germany picked up at the U.N. last month and are continuing, according to officials briefed on the diplomacy. But they have been complicated by differences among the allies over the timing and terms.

The attraction of the initial deal, U.S. officials said, was that Iran wouldn't have been left with enough nuclear material to produce an atomic weapon.

Iran has grown its supply of low-enriched uranium over the past year to roughly 2,800 kilograms from around 1,800 kilograms as of September, according to the U.N.'s nuclear watchdog body, the International Atomic Energy Agency. Iran has also begun producing low-enriched uranium at levels closer to weapons-grade.

U.S. officials said the current talks are focused on securing a much larger amount of Iran's nuclear-fuel stockpile. The U.S. also is seeking to build on the fuel-swap arrangement that Iran reached with Turkey and Brazil in May. That called for Iran to ship out 1,200 kilograms of low-enriched uranium for conversion into fuel rods for the Tehran reactor, but didn't address U.S. fears about Iran enriching uranium further. "Any revised approach would have to address the deficiencies that the U.S. and other P5+1 countries have pointed out in the proposal made by Iran, Turkey, and Brazil in May," said a senior U.S. official involved in the diplomacy.

Other formulas continue to be discussed to secure a larger amount of Iran's stockpile of low-enriched uranium, according to the three officials briefed on the diplomacy. One would see a portion of Iran's low-enriched uranium stock, which is stored as a gas, converted into uranium oxide, a powder. Such a procedure could delay by months any Iranian effort to produce weapons-grade fuel, as the uranium oxide would have to be converted back into a gas.

The U.S. and its negotiating partners have also discussed allowing Iran to store its stockpile of low-enriched uranium in another country, such as Turkey. Tehran signed on to this provision in its May agreement with Turkey and Brazil. But the U.S. objected to Iran's ability to bring the nuclear fuel home without the approval of the IAEA or the international community.

The U.S. and its allies hope to meet with Iranian officials November 15-17 to discuss both the fuel-swap arrangement and broader international concerns over Iran's nuclear program.

"A revised arrangement cannot be a substitute for addressing our core concerns or the requirements of U.N. Security Council and IAEA resolutions," the U.S. official said. "It's a modest step to improve confidence."

Iranian officials on Tuesday said there hasn't been any agreement yet on a formal agenda for the talks. "Discussions are under way about the date of the negotiations, the venue and content of the negotiations," Foreign Ministry spokesman Ramin Mehmanparast told reporters in Tehran.

Mr. Ahmadinejad has said that in any future talks the international community must acknowledge Iran's rights to develop nuclear fuel and address the issue of Israel's assumed nuclear-weapons arsenal.

UNCLASSIFIED

19. Iran Begins Loading Fuel at Nuclear Reactor

William Yong and Alan Cowell, New York Times, 27 October 2010, Page A8

TEHRAN -- Iran on Tuesday celebrated the start of the process of loading 163 fuel rods into the core of its first nuclear power plant reactor, putting it within months of operation.

The Bushehr reactor, cast by Tehran as a showcase of its peaceful nuclear intentions, is separate from other more contentious operations elsewhere in the country where Iran is seeking to enrich uranium. But the timing is delicate in diplomatic terms, as tighter sanctions are being put in place against Iran by the United Nations Security Council, the United States and the European Union.

Iran has not yet formally responded to an invitation to join international powers for talks on its nuclear program in Vienna in mid-November.

In Iran, Ramin Mehmanparast, a Foreign Ministry spokesman, said Tuesday, "Political pressure and sanctions have not prevented Iran from proceeding with its peaceful nuclear activities according to schedule."

"The Bushehr power plant is a major project which will help us to take one step toward future alternative energy supplies," he said, according to the semiofficial news agency IRNA. "We will also pursue our peaceful nuclear activities in other areas."

Iran has five research reactors in operation, and one more under construction.

The Bushehr reactor, designed for power generation and located in southern Iran, has a long and tangled history. Construction began in 1975 under a contract signed with West Germany, state-run Press TV reported on Tuesday, but West Germany withdrew from the project after the Islamic Revolution in 1979. An agreement with Russia in 1995 should have been completed in 1999, but the plan fell prey to long delays.

The United States once opposed the plant. But the International Atomic Energy Agency monitors it, and the United States dropped its objections after Russia provided assurances of controls on the fuel supply and the disposal of spent fuel rods. Russia has agreed to take back the spent rods, removing the possibility that Iran could reprocess them for materials that could fuel a nuclear weapon.

Secretary of State **Hillary Rodham Clinton** reiterated Tuesday that the United States was not concerned with the Bushehr plant but with other sites.

"Our problem is not with their reactor at Bushehr, our problem is with their facilities at places like Natanz and their secret facility at Qum and other places where we believe they are conducting their weapons program," Mrs. Clinton told reporters at the United Nations, according to The Associated Press.

"Iran is entitled to the peaceful use of nuclear power," she added. "They are not entitled to a nuclear weapons program."

The Iranian government maintains that its program is for energy production and other peaceful uses. But with Iran having hidden elements of the program in the past and making no secret of its ambitions to increase its regional power, Western governments harbor deep suspicions that Tehran wants to build a nuclear weapon.

The fuel loading was initially planned to begin soon after fuel was transported there in August, but was delayed by what the Iranians said was a leak in a pool near the central reactor. Iranian officials have denied that the delay was caused by the mysterious Stuxnet computer worm, which was found on the laptop computers of several employees at Bushehr, as well as a power generator that is not believed to be part of a weapons program.

Speaking to workers at the plant on Tuesday, the head of Iran's Atomic Energy Organization, Ali Akbar Salehi, called the Bushehr plant "the most exceptional power plant in the world."

He said that the plant would begin to feed the national power grid within three months.

Normal procedures call for I.A.E.A. inspectors to oversee the final processes of fuel-loading and then seal the core of the reactor to prevent tampering. The reactor is to be kept under surveillance by closed-circuit television cameras that would detect any movement of fuel.

But in September, the I.A.E.A. complained that Iran had barred two of its most experienced inspectors from the country.

In a report, the agency reiterated that, since August 2008, Iran has refused to answer questions "about the possible existence in Iran of past or current undisclosed nuclear-related activities involving military-related organizations, including activities related to the development of a nuclear payload for a missile." The report said it was "essential that Iran engage with the agency on these issues" because evidence can degrade with "the passage of time."

William Yong reported from Tehran, and Alan Cowell from London. William J. Broad contributed reporting from New York.

UNCLASSIFIED

20. Teenage Recruit Joins Jihad

Would-Be Suicide Bomber in Karachi Tells of Pakistan Taliban Indoctrination

Tom Wright and Owais Tohid, Wall Street Journal, 27 October 2010, Page A15

KARACHI, Pakistan -- The recruitment described by a 14-year-old alleged terrorist in this teeming port city shows the growing spread of a web of extremist groups in the region.

On Monday, Mohammad Salaam and two alleged members of the Pakistan Taliban, which is locked in a two-year-old war with the Pakistani state, were arrested by police as they allegedly prepared a suicide attack.

In an interview at a Karachi police station, with policemen present, Mr. Salaam described a short path to becoming a suicide bomber. "They would brainwash me by talking about jihad all the time," he said of his Pakistan Taliban minders. "I could feel it in my soul."

Mr. Salaam remains in detention, but hasn't been charged. Police said he will be released because he is a minor.

The Pakistan Taliban, which operate chiefly from remote tribal areas, have been able to forge deep ties in this city of 18 million, and in other cities and towns, through connections with local Islamist extremist groups that procure funds and recruit would-be suicide bombers.

Those bonds are one reason the Pakistani military is reluctant to act on mounting pressure from the U.S. to broaden its war in the tribal regions in the northwest of the country. U.S. officials say an offensive in the North Waziristan tribal region is needed to root out Afghan Taliban and allied groups that attack U.S. troops over the border in Afghanistan.

But Pakistan's military says such an operation would be met by an escalation of attacks by Pakistan Taliban and its allies, unleashing retaliatory strikes in Karachi and other major urban centers they have infiltrated across the country.

"There would be a wave of suicide bombings across Pakistan," said Gen. Athar Abbas, the military's chief spokesman.

After the current offensive against the Pakistan Taliban began two years ago, the group retaliated with attacks in several cities against government, police and military targets, as well as shrines seen by extremists as heretical.

The Pakistan Taliban claimed responsibility for an attack this month on Karachi's revered Abdullah Shah Ghazi shrine, which killed eight people. An attack Monday on a shrine in southern Punjab killed five.

The group has also attracted recruits from outside Pakistan. The failed Times Square bomber, Faisal Shehzad, said he trained in North Waziristan with the Pakistan Taliban.

Links between the Pakistan Taliban, a network of militants mainly from the Pashtun Mehsud tribe of South Waziristan, and extremist groups in Karachi have deepened in recent months, local police say.

One of the men arrested on Monday, Sher Rehman, was an operative with the extremist group Lashkar-e-Jhangvi who worked for the Pakistan Taliban, police officials said.

Lashkar-e-Jhangvi began in the 1990s in Pakistan's eastern Punjab province as a Sunni sectarian group targeting minority Shiites. Pakistan banned the group, along with a number of others, under U.S. pressure in 2001. Its fighters, largely ethnic Punjabis, many of whom had fought in Afghanistan and against Indian troops in Kashmir, sought shelter in the tribal regions, deepening bonds with the Taliban on both sides of the border.

It was Mr. Rehman's job to recruit fighters among Karachi's youth and to extort money from local businesses to provide funding, police said.

On Monday, police stormed a house in Sohrab Goth, a Pashtun area in the northern suburbs of Karachi, arresting Mr. Salaam, Mr. Rehman and a third person. Three others escaped after a gun battle.

Police said they found a suicide jacket with 48 pounds of explosives buried in the garden.

Mr. Salaam, a Karachi-born ethnic Mehsud Pashtun with downy hair on his upper lip and acne on his cheeks, said that until a few months ago his favorite pastime was playing "Counter-Strike," a videogame in which terrorists take on law-enforcement agencies.

Mr. Salaam's family—he has five brothers and his father drives a mechanized excavator—has no history of militant violence, police said. At school in Sohrab Goth he enjoyed studying sciences and computer studies, he said.

He said he was approached by a local vegetable seller, an ethnic Afghan member of the Pakistan Taliban, who urged him to carry out jihad.

He heard stories about U.S. troops carrying out atrocities against Pashtuns in Afghanistan and developed a conviction to attack U.S. soldiers there. "I wanted to blow up the American army. I hate American troops," he said.

He was introduced to Mr. Rehman after Eid-ul-Fitri, the Muslim holiday, in September. The recruiter, he said, persuaded him instead to strike in Pakistan, telling him, "the reward is the same."

The reward he was promised, he said, was eternal peace in heaven.

He said Mr. Rehman threatened to kill him if he told anyone about his mission.

Copyright 2009 Dow Jones & Company, Inc. All Rights Reserved

[Back To Table Of Contents](#)

UNCLASSIFIED

21. Saudi Border With Yemen Is Still Inviting for Al Qaeda

Robert F. Worth, New York Times, 27 October 2010, Page A1

ON THE SAUDI-YEMENI BORDER -- The five Yemeni men, all of them rail-thin, clutched their knees as they sat staring across the sand at the narrow road, which separates the Arab world's poorest country from its richest.

"They're waiting for us to move on," said the Saudi border guard with a weary smile, as he sat watching from the front seat of a gleaming S.U.V. "Waiting so they can try to cross."

This remote 1,100-mile frontier, once a casual crossing point for Bedouins and goats, has become an emblem of the increasingly global threats emanating from Yemen: fighters from Al Qaeda, Shiite insurgents, drugs and arms smuggling and, well under the world's radar, one of the largest flows of economic refugees on earth.

Every day hundreds of illegal migrants are caught and sent back to Yemen, Saudi officials say, including many who have come from Africa and across Yemen's deserts fleeing war and hunger.

The porousness of the border is essential to Al Qaeda's Yemen-based branch, which has become a major terrorism concern for the United States as well as Arab countries. Al Qaeda draws recruits from Saudi Arabia, where they can cross and recross without being noticed, and it has sent militants across to try to kill Saudi leaders in their efforts to topple the oil-rich kingdom.

In response, the Saudi authorities have embarked on a multibillion-dollar effort to strengthen the border, evacuating scores of villages that once straddled it and building elaborate defense networks to keep intruders out.

Earthen berms now prevent cars from crossing, and layers of concertina wire line the roads, some of it strewn with the rags and dried blood of desperate migrants who still try to get through. Floodlights and thermal cameras focus on different parts of the border at night, and intelligence units stand ready to interrogate anyone who is deemed suspicious.

"They adapt very quickly to every strategy we have," said Lt. Muhammad Qahtani, a seven-year veteran of the border patrol. The migrants wear their shoes backward to confuse trackers, or strap sponges to their soles to leave no footprints at all. They trek through arid mountains where the border is loosely patrolled.

Many smugglers are heavily armed and will fight to the death when surrounded, Lieutenant Qahtani said, because they know convicted drug traffickers are usually beheaded in Saudi Arabia.

In some ways the border here resembles the one separating the United States from Mexico, another desert barrier between rich and poor nations.

But this border has become far more volatile lately. A year ago Yemeni rebels killed a Saudi border guard, setting off a short war that delivered a humiliating blow to the Saudis' well-financed but inexperienced military.

At least 133 Saudi soldiers were killed over three months, and the fighting raised alarms across the Sunni Arab world about the possibility that Iran might be supporting the Yemeni rebels -- who subscribe to an offshoot of Shiite Islam known as Zaydism -- and turning this border into another front for sectarian conflict.

Al Qaeda's Yemen-based branch has repeatedly boasted about its ability to infiltrate the border and outwit Saudi Arabia's network of informants in the area. Last year, a suicide bomber crossed here and later came close to assassinating Prince Muhammad bin Nayef, who runs Saudi Arabia's counterterrorism efforts. In October 2009, Yusef al-Shihri, a leading Qaeda operative who had been detained at Guantánamo Bay, was killed in a gun battle after crossing the border from Yemen disguised as a woman.

Border security here involves far more than fences and patrols. Some tribes straddle the border, and they -- and the Yemeni government -- protested fiercely when Saudi Arabia first began reinforcing the border in 2003, saying they needed free access for grazing. That dispute seems to have eased, and the Saudi government is now refining an old policy of subsidies to border tribes with a view to security, analysts say.

"The Saudis realize they need to work with tribal leaders and make sure their livelihood depends on how good they are at keeping the border safe," said Bernard Haykel, a professor of Near Eastern Studies at Princeton who has written extensively on Yemen and Saudi Arabia. "There's also cross-border trade, and there is a debate inside Saudi Arabia now on how hard the border should be."

In the past, many Yemenis complained that Saudi Arabia's support for various tribal and political figures in Yemen seemed aimed at keeping their southern neighbor divided and weak. Now, as Yemen's instability and the threat of terrorism grow worse, Saudi Arabia appears to be reassessing its approach to Yemen and its longtime president, Ali Abdullah Saleh, diplomats say.

"They are trying to be more systematic," said a Western diplomat in the Saudi capital, Riyadh. "Their manipulations are now aimed at supporting Saleh, because he's the only game in town."

The border was officially demarcated only in 2000. Much of it remained so informal that many villages on the border's western edge, near the Red Sea, were half-Yemeni, half-Saudi. Those days ended last year with the war, when the Saudi government evacuated 78 border villages and extended the network of fences it had begun building several years earlier.

The area is an eerie wasteland now -- scores of houses, some of them pockmarked with bullets from the war, sit empty and silent. At the top of the mountain where the fighting started last year, Saudi soldiers man a .50-caliber machine gun, gazing across at the unmarked ridges that form the border with Yemen.

Inside the border patrol headquarters in the port city of Jizan, photographs line the wall showing contraband captured by the patrol guards: truckloads of rocket-propelled grenades, huge bricks of hashish, stacks of machine guns.

Drug smuggling has risen by almost a third in the past two years, Saudi officials in Jizan say, with more than 7,000 pounds of hashish seized so far this year. The most dangerous smugglers of all are those who drive through the Empty Quarter, the Texas-size sand desert that dominates the southern part of the Arabian Peninsula, patrol officers say.

But far more numerous are the illegal migrants, hundreds of thousands of them annually in recent years. Most are caught and sent back to Yemen after being held in crowded border detention centers for a day or so. Many have crossed the sea to Yemen from Somalia or Ethiopia, risking death on rickety boats in shark-infested waters. Most of the survivors make the arduous journey through Yemen's arid mountains only to be turned back at the Saudi border.

"Some of them say, 'If you give me something to eat, I will go back,' " said Lieutenant Qahtani, the border patrol officer. "You can only feel pity for these men."

Copyright 2010 The New York Times Company

[Back To Table Of Contents](#)

UNCLASSIFIED

22. Yemeni journalist on trial for Qaeda, Awlaki links

** Shai accused of trying to recruit for al Qaeda*

** Defence lawyers boycott trial*

Reuters.com, 26 October 2010

SANAA, Oct 26 (Reuters) - A Yemeni journalist and expert on al Qaeda is being tried for alleged links to the global militant group, including helping to publicise the views of a U.S.-born Muslim cleric wanted by Washington.

The trial of Abdulelah Shai started on Tuesday in a special security court not attended by his lawyers, who like several attorneys in Yemen, consider the court illegal and boycott it.

Shai's interview with radical preacher Anwar al-Awlaki, who has been linked to the failed bombing of a U.S.-bound plane in December 2009, was posted on the website of Al Jazeera television earlier this year.

Prosecutors accused Shai of "being an active al Qaeda member, including acting as a media secretary for the radical Muslim preacher and working to attract a number of foreigners into joining al Qaeda". His defence team denies the charges.

"Everything Shai did was part of a journalist's job of seeking information, whether this is information the government likes or not," said Mohamed Allawo of the National Organisation for Defending Rights and Freedoms, which is defending Shai.

Shai has made numerous appearances in international media as an al Qaeda expert and is often described as having a close relationship with members of the militant group.

"There is no real charge, because there's no case in the Yemen judiciary against Anwar al-Awlaki and there is no ruling that criminalises contact with Awlaki," Allawo said.

The U.S. Treasury has blacklisted Awlaki as a "specially designated global terrorist", a move that freezes any assets he may have under U.S. jurisdiction.

Earlier this year, the United States authorised the CIA to capture or kill him. Awlaki has been linked to an army major who went on a shooting spree that killed 13 people last year at Fort Hood in Texas.

Impoverished Yemen, neighbour to top oil exporter Saudi Arabia, has been under international pressure to quash a resurgent regional wing of al Qaeda based in the country.

The government has been mounting a U.S.-backed crackdown against the militants since the Yemen branch claimed responsibility for the failed December plane bombing.

In July, Shai was snatched off the streets of Sanaa by agents who interrogated him about al Qaeda and briefly detained him. He was arrested and imprisoned on Aug. 16.

Last month, the Committee to Protect Journalists called on Yemen to release Shai, criticising the country for what it said was a crackdown on the media. (Reporting by Mohammed Ghobari; writing by Erika Solomon; editing by Andrew Roche)

© Thomson Reuters 2010. All rights reserved.

[Back To Table Of Contents](#)

UNCLASSIFIED

23. In Mideast House of Cards, U.S. Views Lebanon as Shaky

Mark Landler, New York Times, 27 October 2010, Page A4

WASHINGTON – The Obama administration, already struggling to stave off a collapse of Middle East peace talks, is increasingly alarmed by unrest in Lebanon, whose own fragile peace is being threatened by militant opponents of a politically charged investigation into the killing in 2005 of a former Lebanese leader.

With an international tribunal expected to hand down indictments in the assassination of the former prime minister, Rafik Hariri, in the coming months, the Hezbollah militia is maneuvering furiously to halt the investigation, or failing that, to unseat Lebanon's government, which backs it.

The White House sent a senior diplomat to Beirut last week to reassure Lebanon's president, Michel Suleiman, of President Obama's support for the investigation and his country's stability. The visit by the diplomat, Jeffrey D. Feltman, the assistant secretary of state for Near Eastern Affairs, came on top of a telephone call to Mr. Suleiman by Secretary of State **Hillary Rodham Clinton**.

"The president felt very strongly that we need to reconfirm our commitment to Lebanon's independence, Lebanon's sovereignty and Lebanon's stability," Mr. Feltman said in an interview. "There are people inside Lebanon who are arguing that it faces a choice of justice versus stability. That's an artificial choice."

The administration's worries go beyond Lebanon itself, and help explain why it, and not the stalled Israeli-Palestinian negotiations, has been the major preoccupation of American foreign policy officials for the last few weeks.

The diplomatic activity follows a splashy tour of Lebanon by Iran's president, Mahmoud Ahmadinejad, who got an ecstatic reception from members of Hezbollah, the Shiite movement financed and equipped by Iran. American officials were particularly struck by Mr. Ahmadinejad's trip to a small town a few miles north of the Israeli border, where he called for the "Zionists to be wiped out."

Lebanon has long been a proxy state for battles between adversaries in the Middle East, and Iran's attempts to build influence there are not new. But at a time when the United States is trying to revive peace talks, administration officials concluded that Iran's latest muscle-flexing could not go unanswered.

"You don't want the perception of a vacuum," Mr. Feltman said. "You don't want the perception that Ahmadinejad is the only game in town."

Analysts said that the United States was right to reassert its commitment to Lebanon, but that it may be acting too late. Rising prices for weapons suggest that militias other than Hezbollah are rearming, increasing the threat of a civil war.

There are limits to what the administration can do to stabilize a country as divided as Lebanon. The United States has given the Lebanese armed forces \$670 million in military aid since 2006. But last August, several members of Congress put a hold on further funds after a skirmish between Lebanese and Israeli soldiers raised suspicions that parts of the Lebanese Army were in league with Hezbollah.

Mr. Ahmadinejad's jubilant reception in Lebanon has only added to the resistance on Capitol Hill. Representative Eliot L. Engel, a Democrat from New York who sponsored a bill imposing sanctions on Syria, said he would consider voting to block aid because of fears that it could end up helping Hezbollah.

"We need to be careful about what we do there, so we're not strengthening the hand of a terrorist group like Hezbollah and its allies," Mr. Engel said in an interview. "We just don't want to use our monies to enhance policies that are bad for Americans and bad for the people of Lebanon."

The Special Tribunal for Lebanon was sanctioned by the United Nations Security Council in 2007 to investigate the car bombing that killed Mr. Hariri and 22 others in February 2005. Lebanon's coalition government, now led by Mr. Hariri's son, Prime Minister Saad Hariri, has pledged to contribute 49 percent of the tribunal's expenses and enforce its judgments.

The Netherlands-based tribunal has been at work since March 2009, but has said little about when it plans to hand down indictments.

A raft of reports in Lebanon's news media said an announcement could come as early as December, though some reports now suggest that the tribunal may not act until the first quarter of next year.

In either case, a sense that the investigation is entering its final stages has contributed to a feverish political environment.

The trouble is, those indicted may include members of Hezbollah, and the group, which holds seats in the Lebanese cabinet, is demanding that Prime Minister Hariri disavow the investigation. Syria, also under suspicion for having a role in Rafik Hariri's assassination, has taken up calls to discredit the tribunal.

Syrian officials, who had once backed Saad Hariri's government, are now sharply critical of him and his March 14 alliance, a coalition that grew out of the "Cedar Revolution," which pushed Syrian troops out of the country. Al Akhbar, a Lebanese newspaper that is closely allied with Hezbollah and Syria, declared recently that "taking authority away from Hariri would teach him how to keep it."

Saudi Arabia has tried to mediate, without much success. American officials say they believe that the tribunal will be able to complete its investigation. But their concern is that indictments will draw protesters onto the streets, inflaming tensions between Shiite and Sunni factions. Unrest could also lead to fresh skirmishes between Lebanese and Israeli forces along the border between the countries.

That would imperil a peace effort that is already on life support. Prime Minister Benjamin Netanyahu's chief negotiator, Yitzhak Molcho, has been in Washington for the last few days, officials said, floating various ideas on ways to revive the talks. But there is no indication of an imminent breakthrough.

Syria's increasingly disruptive role is also raising questions about the Obama administration's 18-month effort to engage that country. Some analysts said it was time for the administration to rethink that effort.

"This is the moment when we need a straight answer out of Syria," said Andrew Tabler, an expert on Syria and Lebanon at the Washington Institute for Near East Policy. "They just seem unwilling or unable to deliver it."

Copyright 2010 The New York Times Company

[Back To Table Of Contents](#)

UNCLASSIFIED

24. Turkey in Dilemma Over NATO Shield

Marc Champion, Wall Street Journal, 27 October 2010, Page A13

ISTANBUL -- Turkey's top security body is set to discuss Wednesday whether to back a U.S.-led plan to build a missile-defense shield against rogue states—a moment that could force Ankara to choose between its longstanding westward orientation and its recent courtship of Iran.

The National Security Council, which consists of top military commanders and political leaders, is expected to debate the North Atlantic Treaty Organization's proposal for a defense shield largely built and funded by the U.S. A senior Turkish diplomat said Ankara will have to decide its position before next month's summit of the 28-nation alliance in Lisbon, Portugal, where Turkey and other NATO members are due to decide whether to go ahead with the plan.

For most NATO members, the shield is an insurance policy against a potential missile threat from Iran. It is also a welcome compromise from the much more ambitious plan of the previous Bush administration. That proposal, which would have installed antiballistic missiles in Poland and a forward radar system in the Czech Republic, triggered a fierce backlash from Moscow.

For Turkey, however, the Obama administration's scaled-back plan is proving a major diplomatic headache that risks forcing Ankara to choose between NATO and Iran. It is also triggering a fierce debate inside the country over where Turkey's core interests lie. In recent days, Turkey's religious conservative and pro-government media have argued that siding with NATO against Iran would end Turkey's effort to build an independent foreign policy and damage its credibility in the Middle East.

Both U.S. and Turkish leaders say no decision has yet been made as to which countries will host the system. Bulgaria, Romania and Turkey are in the picture, according to diplomats familiar with the matter. But Turkey, which shares a border with Iran, is the location of choice for the plan's forward radar, according to military analysts and diplomats.

Turkish leaders have so far remained noncommittal and have asked Washington for assurances and technical details. According to diplomats familiar with the matter, Turkey is asking that NATO not name any specific country as the source of a missile-attack threat. It also seeks to ensure that all of Turkey's territory is covered by the system and that Turkey has access to all data and a measure of control over the decision to fire. These people say Ankara also wants guarantees that non-NATO members, specifically Israel, wouldn't gain access to the data.

"No decisions have been made yet," said the senior Turkish diplomat. "We don't know exactly how this system will be formed, what will be the command and control structure, the threat perception and other issues. So that's why our talks are continuing."

Some of the Turkish requests shouldn't be problematic, said one non-Turkish diplomat familiar with the matter. Command and control of the system would have to be at an operational, not political, level, due to the short time frame available to shoot a missile down. Turkey would therefore have a say--and a potential veto--in setting the rules of engagement. Similarly, other countries, as well as Turkey, are concerned that data should be available only to NATO members, the diplomat said.

"If Iran is not mentioned by name and the shield covers Turkey in its entirety then I think [Turkey's government] will go along with it," said Soli Ozel, a prominent newspaper columnist on international affairs and professor at Bilgi University in Istanbul. "If those conditions are fulfilled and the government still refuses, then all these discussions about Turkey's direction will come back with a vengeance."

Turkey's military wants the shield, according to Huseyin Bagci, professor of international relations at the Middle East Technical University in Ankara. "[Iranian] Sahab missiles can reach any part of Turkey," he said, adding that militaries focus on the capabilities of potential foes, not their intentions.

Indeed, Turkey has a plan of its own to purchase a missile system to protect its borders. Raytheon Co., maker of the Patriot missile, is one of the bidders and earlier this month announced a deal to subcontract part of the Patriot system's manufacture to Turkey's largest arms maker, Aselsan Elektronik Sanayi ve Ticaret AS.

Yet Turkish diplomats are concerned that positioning a NATO missile system on Iran's border would infuriate Iran, a country that supplies about a third of Turkey's energy and which Ankara has worked hard to court, presenting itself as a neutral party in the international dispute over Tehran's nuclear fuel program. A NATO shield also would also cut across the grain of Foreign Minister Ahmet Davutoglu's frequent statements that Turkey doesn't believe it is threatened by any of its neighbors.

Copyright 2009 Dow Jones & Company, Inc. All Rights Reserved

[Back To Table Of Contents](#)

UNCLASSIFIED

25. Iraq al Qaeda more lethal as homegrown insurgency

Suadad Al-salhy, Reuters.com, 26 October 2010

BAGHDAD (Reuters) - Al Qaeda's Iraqi branch has evolved into a homegrown, more lethal and bolder insurgency comprised of Iraqi fighters hardened in U.S. prisons and posing a challenge to Iraqi forces, military officials say.

The insurgency has been strategically weakened by the deaths of leaders, and both its numbers and the territory in which it can maneuver have shrunk since 2006-07, when Sunni tribal chiefs turned on it and joined forces with the U.S. military.

But what Iraqi officials call the "third generation" of al Qaeda in Iraq may be more difficult to fight than before because its fighters can blend in, know the weaknesses of Iraqi society, and are more interested in making a spectacular splash with their attacks than in battlefield victories.

Their assaults are aimed at grabbing attention and rattling the population at a time when sectarian tensions are fraught because of the failure of politicians to agree on a new Iraqi government seven months after an inconclusive election.

"We face the third generation of al-Qaeda now, a generation that mostly graduated from (U.S. detention camps) Bucca, Cropper and other such places," said Major General Hassan al-Baidhani, chief of staff for the Baghdad operations command.

Al Qaeda has shown "a new type of boldness," attacking heavily protected targets and security forces head on, Baidhani told Reuters. "This strategy depends basically on shock. They are not looking for success as much as looking for attention."

Shi'ite Prime Minister Nuri al-Maliki is battling to retain his job, opposed by the Sunni-backed, secular Iraqiya alliance of ex-premier Iyad Allawi and some erstwhile Shi'ite allies.

If Iraqiya ends up being sidelined, the Sunnis who voted for it in March may react in outrage and return to supporting the Sunni Islamist insurgency, security officials say.

In the run-up to the 2003 U.S.-led invasion, the Bush administration accused Saddam Hussein's regime of having links to al Qaeda as part of its campaign to bolster support for war.

No ties were ever proven but al Qaeda was quick to take advantage of the post-invasion chaos to establish a presence in Iraq.

The first generation of al Qaeda on Iraq's battlefields were primarily Arabs from abroad. The second was a mix of foreign and Iraqi Sunnis angered by the invasion and the rise to power of Iraq's Shi'ite majority after the fall of Saddam, Sunni.

Now as Iraqi security forces take center stage after U.S. troops halted combat operations in August prior to a full withdrawal in 2011, they face a homegrown threat composed of young radicals who fervently believe in jihad, or holy war.

WEAKNESS OF SOCIETY

"And therein lies the danger because they know the weak points of Iraqi society," said Baidhani, who has documented al Qaeda activities over the last four years.

On June 13, al Qaeda's Iraqi affiliate, the Islamic State of Iraq, sent a wave of suicide bombers against the well-guarded Central Bank in Baghdad, killing 15 people. The following month, a suicide bomber attacked Saudi-owned al-Arabiya news channel, another well-protected, high-profile target.

On September 5, suicide bombers killed 12 when they swarmed a Baghdad army base, where just two weeks earlier a lone suicide bomber had managed to kill 57 army recruits and soldiers.

The attack on the army base took officials by surprise, said a senior police official who asked not to be named. Up till then, military strategists had believed insurgents would have no success using suicide bombers against military installations.

"The problem is our enemy's intelligence is stronger than our intelligence," the official said. "They know the timings of our duties, food, rest, hours when patrols switch, the type and the number of weapons at our bases."

U.S. military leaders say the transformation of al Qaeda in Iraq coincided with strikes against it, including the killing of its top two leaders Abu Ayyub al-Masri and Abu Omar al-Baghdadi, and the cutting of its links to al Qaeda abroad, this year.

"They have attempted to wean themselves off a foreign leadership structure," U.S. Brigadier General Ralph Baker said.

Al Qaeda cells are trying to move back into strongholds like the districts of Adhamiya and Fadhil in the capital, and distributing threatening leaflets to cow the public.

But the group is unlikely to be able to succeed at its long-term goal of bringing down the government and Iraq's nascent democracy, and establishing a Sunni Islamist caliphate.

"We don't see al Qaeda as an existential threat to the Iraqi government any more," Baker said.

(Additional reporting by Jim Loney, Editing by Michael Christie and Angus MacSwan)

© Thomson Reuters 2010. All rights reserved.

[Back To Table Of Contents](#)

UNCLASSIFIED

26. Saddam aide Tariq Aziz sentenced to death in Iraq

Two others face same fate for persecution, murder

Ashish Kumar Sen, Washington Times, 27 October 2010

Tariq Aziz, Saddam Hussein's former right-hand man and once the international face of the Iraqi regime, was sentenced to death by the Iraqi supreme criminal court on Tuesday.

Aziz, deputy prime minister and foreign minister in Saddam's regime, had been charged with "deliberate murder and crimes against humanity."

Two other defendants in the case, former Interior Minister Sadoun Shakir and Saddam's private secretary, Abid Hamoud, also received death sentences.

All three were sentenced for their roles in the persecutions and murders of members of Prime Minister Nouri al-Maliki's Shiite-dominated Dawa party, including its founder, Mohammed Baqr al-Sadr. The Dawa party was the main opposition group during Saddam's reign.

Aziz, 74, is reported to be seriously ill.

His attorney, Badee Izzat Aref, told the Associated Press that the verdict was "politically motivated."

However, State Department spokesman Michael Tran said all sentencing rulings, including Aziz's death sentence, were "Iraqi decisions reached in accordance with Iraqi law."

"Tariq Aziz has been convicted of numerous crimes against the people of Iraq," Mr. Tran said.

Aziz was also sentenced to 15 years in prison for "committing torture" and 10 years for "participating in torture." The court ordered that all his known wealth be confiscated.

In 2009, Aziz was handed a 15-year prison sentence for the executions of 42 Baghdad merchants in 1992. He also was given a seven-year sentence for his role in expelling Kurds from Iraq's north.

He pleaded not guilty in both cases.

In a phone interview from Dubai, Samer Muscati, a researcher with Human Rights Watch's Middle East division, said the process under which Aziz was tried is "flawed because of serious administrative, procedural and substantive legal defects."

"It is always a concern when someone is sentenced to death under the Iraqi penal system, considering the due process issues that exist," Mr. Muscati said.

Some expressed surprise at the death sentence for Aziz.

While serving as U.S. ambassador to Iraq between 1984 and 1988, David Newton met numerous times with Aziz.

"He was a very intelligent, active and capable foreign minister. Of course, he was working for a totalitarian government, but he favored a relationship with the United States," said Mr. Newton, who is currently with the Middle East Institute.

Mr. Newton said that if Aziz's only role was that he signed some documents ordering the execution of Iraqis on Saddam's orders, his death sentence was not justified.

"Having been in Iraq four years, I know that under Saddam Hussein you did not refuse to do what you were ordered," he said.

Kenneth Katzman, a specialist in Middle Eastern affairs at the Congressional Research Service, said Aziz's death sentence was unexpected.

"There was a feeling that because he is a Christian, he wasn't involved in any of the sectarian human rights abuses, anti-Shia discrimination," Mr. Katzman said.

In fact, he said, Aziz tried to be a moderating influence on Saddam and even opposed the invasion of Kuwait, which triggered the Persian Gulf War in 1991.

The Vatican, meanwhile, urged Iraqi authorities not to execute Aziz, saying leniency would help reconciliation, peace and justice.

Aziz surrendered to U.S. troops after they invaded Iraq in 2003. He later said he regretted that decision.

Aziz's Jordan-based son Ziad told Agence France-Presse that the sentence was "an act of revenge against anybody and anything related to the past."

However, Michael Rubin, a resident scholar at the American Enterprise Institute, said it was ridiculous to think that Aziz was guilty only by association with the Saddam regime.

"This wasn't a man who joined the Ba'ath Party because he wanted an extra \$20 per month. He was part and parcel of one of the most tyrannical regimes of the 20th century, a central decision-maker," Mr. Rubin said.

Describing de-Ba'athification in Iraq as the West's greatest achievement and legacy, Mr. Rubin added: "The Shia and Kurds will cheer Tariq Aziz's execution."

Under Iraqi law, death sentences can be appealed.

Mr. Katzman said the court ruling puts a cloud over the Iraqi justice system. "It calls into question the commitment to rule of law in a post-Saddam Iraq," he said.

"Basically, anyone in the regime has got the death sentence, with a few exceptions," Mr. Katzman said.

In an interview with the Guardian newspaper in August, Aziz said President Obama was "leaving Iraq to the wolves" by withdrawing U.S. troops from the country.

He defended Saddam, saying, "History will show he served his country."

© Copyright 2010 The Washington Times, LLC.

[Back To Table Of Contents](#)

UNCLASSIFIED

27. Anbar Province, Once a Hotbed of Iraqi Insurgency, Demands a Say on Resources

RAMADI, Iraq — As Iraq's political blocs remain unable to form a national government, lawmakers and residents here in Anbar Province are challenging central control of the natural resources within their territory.

The conflict — which pits a Sunni province against a mostly Shiite administration — adds a new battle line in one of the country's most divisive and volatile issues: who controls the vast untapped oil and gas reserves that are necessary to restart Iraq's crippled economy.

The dispute in Anbar Province is over a natural gas field called Akkaz. For more than a year, local lawmakers and tribal leaders courted foreign companies to open the field as part of a regional economic development plan involving power plants and refineries that they say would bring electricity and as many as 100,000 jobs to the region.

But when the national oil ministry auctioned rights to develop the field last week, the sale did not include any of these measures. Residents took to the streets in protest; lawmakers warned that they would not provide security to the winning bidder, a consortium of Korean and Kazakh companies.

"We will not allow the companies to work here unless they take into account our demands," said Qasim M. Abid, the provincial governor. "Not by violence, but we will use legal measures."

Residents stopped just short of threatening unrest.

"Any company that comes by the Ministry of Oil will face many difficulties, because it came despite the will of the people of Anbar," said Mahmud Saleh al-Anima, a merchant in Ramadi.

The province, west of Baghdad, was a hotbed of the Sunni insurgency, and even on a peaceful afternoon, scars of the civil war — bullet holes, shattered buildings — are visible beside signs of oil wealth. Three years of intense sectarian warfare destroyed the region's economy and many of its businesses, schools, roads and other infrastructure. For residents, the main hope for recovery lies in its gas and oil reserves.

But their claim to these resources, like much in Iraq, is open to interpretation. Laws establishing a national energy policy, including revenue-sharing with the provinces, have been stalled since 2007. The Constitution gives the national Oil Ministry authority to negotiate deals — but only in consultation with local governments. The ministry has desperately courted foreign investors, who remain torn between opportunity and the shaky security and political situation.

In Anbar, local officials say they have been ignored for sectarian reasons by the government of Prime Minister Nuri Kamal al-Maliki, which is predominantly Shiite.

"It's our resources, our land, and they never consulted us," said Rabai Mohammed Nail, a member of the provincial council. "Now, all our resources are going to other people. We have no opportunities to work here, no electricity. All benefit should go to our people."

Lawmakers said they would ask the courts to block the sale, though they feared the courts were controlled by Mr. Maliki.

The gas field has become part of the national political fray, with lawmakers from Iraqiya, the multisectarian bloc that won support in Sunni areas, including Anbar, declaring that the auction of Akkaz and other fields was invalid because it was not approved by Parliament. In a statement, the bloc called the auctions "illegal in light of the current constitutional and political vacuum."

Assim Jihad, a spokesman for the Oil Ministry, insisted that the ministry had sole authority to negotiate rights to oil and gas fields like Akkaz, and that the provincial government's negotiation with companies was "against the principle of transparency and openness in the signing of contracts, and this is unacceptable."

But provincial protests can bring development to a halt, said Luay Jawad al-Khateeb, executive director of the Iraq Energy Institute, a nonprofit group that advises the Iraqi Parliament.

"It could be an ugly situation" if local people distrust the deal, he said. "When it comes to implementation, you need the regional authorities and the tribes. Security will come from them."

Other provinces, including oil-rich Basra in the south, have also fought for more control of their resources. At the far extreme, the semiautonomous Kurdistan regional government in the north has freely negotiated more than 20 oil deals in the region. As the national blocs court Kurdish support, the Kurdistan Alliance is insisting on formal recognition of Kurdish rights to the region's resources.

Hajim al-Hassani, a member of Mr. Maliki's State of Law party, took a nationalist line, insisting that all deals and revenue had to go through the central government, then be distributed to the provinces.

"Once you say Kurds have the right to do that, every province will say they have the same right, including Basra," Mr. Hassani said.

But lawmakers in Anbar insisted that they did not want revenue from the field; they just wanted the developers to create jobs in the region.

"The mistake is the Oil Ministry's mistake, not ours," said Jasim M. al-Habousi, chairman of the provincial council. "I believe it's their problem. They have to go back to the contract to change it."

He added that if the consortium did not agree with the provincial government's terms, the Oil Ministry should offer the field again in a later auction. "This is a public request," he said. "It has a very strong base."

UNCLASSIFIED

28. Urban terror threats prompt new UK police training

Paisley Dodds, Associated Press, FederalNewsRadio.com, 26 October 2010

LONDON (AP) -- The British bobby is about to go ballistic.

Faced with growing terror threats involving urban areas, British police are receiving new weapons and specialized training from the SAS, Britain's elite military unit. The hope is that the training and equipment will help if Britain ever faces an attack similar to the 2008 Mumbai shooting spree that killed 166 people and paralyzed India's business capital for days.

Tuesday's announcement comes amid an active European terror threat being tracked by U.S. and European officials. The U.K.'s terror threat rating remains at "severe" - the second highest tier - which means an attack is likely.

News of a possible Mumbai-styled small arms attack emerged last month after the CIA increased strikes in Pakistan to flush out al-Qaida operatives suspected in the plot. Some of the plot's details came from a terror suspect arrested in Afghanistan, intelligence officials have said.

Terror attacks in cities pose multiple challenges - there are more people, increased difficulties in responding because of clogged routes and multiple problems in evacuating crowds.

British officials have refused to comment on whether the plan will arm more of Britain's some 144,000 police officers - a fraction of whom are in armed response units. But they praised the new training.

"We are in a much better place than ever before, with dedicated counterterrorism units based within our regions," a spokeswoman for the Association of Chief Police Officers said, speaking on condition of anonymity in line with departmental policy. "This new training and equipment will put us in an even better position."

Part of the problem in Mumbai was that the first Indian police to respond were armed with little else than sticks and batons while the attackers had AK-47s.

Britain has a deep-rooted tradition of having unassuming and unarmed police - iconic images of bobbies donning their trademark hats and batons.

Although gun crimes are relatively rare in Britain because of tough gun laws, unarmed police struggled for hours last summer to stop a taxi cab driver who went on a shooting spree, killing a dozen people in rural England. Officers said they had to break off their pursuit of the suspect, Derrick Bird, when he turned his gun on unarmed officers.

The new police arsenal will include automatic or semiautomatic weapons that are more powerful and accurate, but Britain's Home Office - which oversees the police - refused to give further details about the types of weapons or how many officers would receive them.

Some U.S. officials have been calling for American police officers to be armed with assault rifles to better prepare for Mumbai-style urban attacks.

Warren Bamford, the special agent in charge of the FBI in Boston, has backed proposals to arm some neighborhood police with the semiautomatic weapons. Boston Mayor Tom Menino had criticized a proposal to arm up to 200 officers with M-16s, saying only specialized police units should have those guns.

The New York Police Department, after studying the Mumbai attack, decided to train reinforcements for its 400 Emergency Service Unit officers who can carry fully automatic Colt M4 rifles. An additional 200 officers have regularly been put through exercises using Mini-14s, a lightweight semiautomatic weapon.

Indian police are also changing their tactics and equipment.

"Mumbai police officers showed tremendous devotion to duty, but they lacked the requisite commando training and equipment to fight the attackers," said K.P.S. Gill, a retired senior Indian police officer with experience in India's counterinsurgency operations.

An inquiry this month into the 2005 suicide attacks in London that killed 52 commuters illustrated just how difficult it was for emergency workers to reach four separate blast sites and the chaos that reigned as everyone tried to determine what was happening.

Militaries around the world have long struggled with urban warfare. "The Battle of Algiers" - a film about France's colonial struggle with insurgents in the Algerian capital - has been used by militants and governments alike as a training lesson in urban combat.

"Most of us have specialized training of some sort, but a situation like Mumbai would be difficult to deal with in London - largely because of how densely populated it is and because of how badly it's congested," a police officer in a specialized unit told The Associated Press. "There would almost certainly be casualties."

He spoke on condition of anonymity because he was not authorized to speak to the media.

The Home Office declined to elaborate on the training, some of which will be taking place at military bases in Britain. The Ministry of Defense would also not comment on the training.

Brian Jones, an American tourist in London, said he believed all the equipment and training in the world wouldn't likely stop an urban attack.

"What happens happens and there is nothing we can really do to stop it," said the 50-year-old from Boston.

But 21-year-old Payal Patel from India had a different view.

"I think increasing security this way is absolutely necessary," she said. "We need to do what we can to prevent any future attacks."

Associated Press writers Ashok Sharma contributed to this report from Delhi, Tom Hays from Manhattan and Gillian Smith from London.

Copyright 2010 The Associated Press. All rights reserved.

[Back To Table Of Contents](#)

UNCLASSIFIED

29. In Russia, corruption has taken on a life of its own

Will Englund, Washington Post, 27 October 2010, Page A12

MOSCOW - In Russia, the greased palm has overtaken the strong hand. For the past decade, Vladimir Putin, now the prime minister, has been building a tightly centralized, practically unaccountable political structure - a structure that tolerates and is highly susceptible to corruption. But now that corruption appears to have expanded beyond the Kremlin's control.

The current president, Dmitry Medvedev, is anxious to deepen Russia's economic relations with the West after the battering of the 2008 financial crisis. He has brought Russia to the doorstep of the World Trade Organization. This month, he led California Gov. Arnold Schwarzenegger (R) and an American delegation to a new school of management that he hopes will spawn Russia's version of Silicon Valley. On Tuesday, he chaired a meeting in the central Russian city of Naberezhnyye Chelny on ways to improve the country's economic efficiency.

But corruption ties an anchor to all his plans.

"Corruption is not a disease, it's a pain. It's a signal that something is not working efficiently," Georgy Satarov, head of the Indem Foundation in Moscow, said Tuesday.

That signal grew stronger Tuesday with the release of the 15th annual Transparency International report on corruption perceptions around the world, ranking nations from least to most corrupt. Russia slid from 146th place to 154th, out of 178 countries, and into a tie with Tajikistan, Papua New Guinea and several African nations.

"How can a country claiming to be a world leader be in such a position?" asked Yelena Panfilova, director of the Moscow office of Transparency International. "It's a situation of national shame."

There is, she said, a "catastrophic gap" between civil society and "state sabotage." Corruption is everywhere - in hospitals and in schools, in utilities and courts, and especially in the ranks of the traffic police - but she said Russia is falling ever more deeply down the international list because of a sense of immunity in the higher levels of government.

According to the report, Russia was the most corrupt among the G-20 nations. The United States, because of financial scandals, dropped out of the top 20 least-corrupt nations for the first time since Transparency International began issuing its annual list 15 years ago. The United States fell from 19th place to 22nd, behind Chile.

In October, Medvedev launched a "Forward, Russia" campaign to fight corruption. But in July, he acknowledged that it had achieved no results. He laments that government ministers do not carry out his orders - the direct consequence, according to Yuli Nisnevich, chief researcher for Transparency International in Moscow, of a corrupt bureaucracy over which the external controls no longer hold sway.

There is no shortage of laws, instructions, orders or publications against corruption, Panfilova said. "But they don't work."

Russian government officials and officeholders routinely list only their government salaries on financial disclosure forms, and yet, Panfilova said, more than a few are able to afford villas abroad and Ferraris at home.

Nearly 80 percent of Russians say that corruption is a major problem and that it is much worse than it was 10 years ago, said Denis Volkov, who analyzes polling data for the Levada Center in Moscow. A majority say Medvedev is right about the problem of corruption and think he is sincere about it. But 71 percent in the most recent poll say any government efforts to fight corruption will amount in the end to window dressing.

Russia has a long history of pulling strings and trading favors. "What do you mean by corruption?" asked Yevgeny Kovtun, a 48-year-old businessman. "I can help one man; after that, he helps me. Is that corruption? No, that's business."

But now corruption has been monetized. Satarov calculated in 2005 that corruption amounted to \$316 billion that year, or more than Russia's federal budget. He thinks it has grown since then.

Corruption has become a nearly insurmountable obstacle to Russia's economic development, he said. "We need real political competition, strong opposition, restoration of the separation of powers, influential media and social organizations that are free to operate. In the current political situation, Medvedev is doomed to failure."

Sergei Markov, a political analyst and member of the lower house of parliament from the ruling United Russia party, said Russia's leaders have been tentative about fighting corruption because they don't want to upset the stability that the country has finally achieved. "Instability is the main threat to economic growth," he said. "And corruption is not contradictory with economic growth."

Medvedev should fire the most corrupt governor every month, he said - imagine how that would concentrate the minds of the others. But Markov was disdainful of global rankings and skeptical about the costs of corruption.

"Investors won't pay attention to Transparency International," he said. "They pay attention to their own experience. Some of them are quite cynical. For some of them, corruption is good."

Special correspondent Alexander Tsymbal contributed to this report.

© 2010 The Washington Post Company

[Back To Table Of Contents](#)

UNCLASSIFIED

30. Gorbachev Says Putin Obstructs Democracy

Clifford J. Levy, New York Times, 27 October 2010, Page A8

MOSCOW -- Mikhail S. Gorbachev, who once supported Prime Minister Vladimir V. Putin, is voicing growing frustration with Mr. Putin's leadership, saying that he had undermined Russia's fledgling democracy by crippling the opposition forces.

"He thinks that democracy stands in his way," Mr. Gorbachev said.

"I am afraid that they have been saddled with this idea that this unmanageable country needs authoritarianism," Mr. Gorbachev said, referring to Mr. Putin and his close ally, President Dmitri A. Medvedev. "They think they cannot do without it."

In an interview, Mr. Gorbachev even described Mr. Putin's governing party, United Russia, as a "a bad copy of the Soviet Communist Party." Mr. Gorbachev said party officials were concerned entirely with clinging to power and did not want Russians to take part in civic life.

Mr. Gorbachev was especially disparaging of Mr. Putin's decision in 2004, when he was president, to eliminate elections for regional governors and the mayors of Moscow and St. Petersburg. Those positions are now filled by Kremlin appointees. The impact of this change was illustrated in Mr. Medvedev's dismissal last month of Moscow's longtime mayor, who was replaced with a Putin loyalist.

"Democracy begins with elections," Mr. Gorbachev said. "Elections, accountability and turnover."

Mr. Gorbachev, the last Soviet leader, was giving interviews this month to promote a benefit concert that his foundation is sponsoring in March in honor of his 80th birthday. The foundation runs a research center and has raised millions of dollars for charities for children with cancer.

Mr. Gorbachev's criticism of Mr. Putin, while not new, appears to have grown somewhat sharper recently, as if Mr. Gorbachev feels that he put Russia on the path toward being a functional democracy, only to have Mr. Putin block its progress.

Neither Mr. Putin nor Mr. Medvedev has responded publicly to Mr. Gorbachev. Asked on Tuesday about Mr. Gorbachev's comments, Mr. Putin's spokesman, Dmitri S. Peskov, seemed to choose his words carefully. "We do feel the deepest respect toward Mikhail Gorbachev, and we certainly respect his point of view," Mr. Peskov said. "But that doesn't mean that we agree with it."

Mr. Peskov said opposition parties had failed to make gains in Russia because their leaders were unpopular and had not developed attractive platforms. "Neither Putin personally nor United Russia as a political party can be held responsible for the inability of other parties to produce anything promising for citizens of this country," he said.

Nursing a sore throat, Mr. Gorbachev spoke with vigor and seemed hardly slowed by age. He met with reporters at his foundation headquarters in Moscow, which is filled with hundreds of photographs and other memorabilia that highlight his efforts to reform the Soviet Union.

Still, nearly two decades after the Soviet collapse, Mr. Gorbachev occupies an awkward place in Russian society. He is arguably more respected abroad than at home, in part because some here blame him for ushering in the political and economic chaos of the 1990s. It is notable that the benefit concert for his foundation will take place at the Royal Albert Hall in London, not in Moscow.

Mr. Gorbachev, who oversaw the Soviet withdrawal from Afghanistan, offered his observations about the current NATO mission in that country, saying that success there was impossible for an occupier. "It would be necessary to exterminate people," he said, emphasizing that that was obviously not an option.

Mr. Gorbachev has recently dabbled in opposition politics. He is part owner of the country's leading opposition newspaper, Novaya Gazeta, several of whose reporters have been killed or wounded in attacks. He tried to help form a political party to compete in parliamentary elections next year, but gave up in the face of daunting legal hurdles.

"For those who want to change the country in order to advance these processes faster, advance democratic processes, the participation of people is needed," he said. "It is necessary to have parties. But go and try to register a party!"

Mr. Gorbachev would not say whom he would endorse for president in 2012. Mr. Putin, who became prime minister in 2008 after he was barred from running for a third consecutive term as president, is thought to be weighing a return to the presidency.

"Russia has a long way to go to usher in a new system of values, to create and provide for the proper functioning of the institutions and mechanisms of democracy – the institutions of civil society," Mr. Gorbachev said. "All this is done through a major transformation in people's brains. And this, clearly, is changing very slowly."

Copyright 2010 The New York Times Company

[Back To Table Of Contents](#)

UNCLASSIFIED

31. Europe amplifies objections to U.S. data-sharing system

Edward Cody, Washington Post, 27 October 2010, Page A13

BRUSSELS - The Obama administration has encountered mounting resistance in Europe to its demands for broad sharing of airline passenger data and other personal information designed to spot would-be terrorists before they strike.

Europe's objections, based on privacy considerations, worry U.S. counterterrorism officials because computer scrutiny of passenger lists has become an important tool in the struggle to prevent terrorists from entering the United States or traveling to and from their havens. The would-be Times Square bomber was hauled off a Dubai-bound airliner in May, a senior U.S. counterterrorism official said, after his name on the manifest produced a ding in **Department of Homeland Security** computers.

European privacy advocates have criticized the U.S. effort to scoop up as much information as possible on U.S.-bound travelers, saying it violates Europe's traditionally stringent data privacy laws. But their power to criticize was boosted recently to the power to block. Since Dec. 1, the European Union's Lisbon Treaty has given authority over such accords to the European Parliament, where privacy concerns are embraced.

"The administration can't just stiff-arm them anymore," said Marc Rotenberg, who heads the Washington-based Electronic Privacy Information Center and testified at a European Parliament hearing in Brussels on Monday.

As a result of lawmakers' concerns, the E.U. executive has demanded a renegotiation of the four-year-old agreement that lays out the conditions under which European airlines can supply passenger data. The move amounts to a recognition that the current accord, renegotiated after the European Court of Human Rights struck down the first version, could never be approved in the European Parliament as it stands.

The negotiations for a new deal, due to get underway in coming weeks, will be conducted by the E.U.'s executive commission, which in the past has been more amenable than the parliament to U.S. concerns. The 27 E.U. heads of state are scheduled to approve the commission's negotiating mandate at a summit conference in December. But privacy advocates have said that regardless of what the heads of state decide, there is a majority in parliament that will reject any accord that does not meet their concerns.

"Now we have the power, and they have to deal with us," said Sophie in 't Veld, a Dutch privacy advocate and European Parliament member who is vice chairman of the Committee on Civil Liberties, Justice and Home Affairs.

Recognizing the new reality, the U.S. mission to the European Union has strengthened its team focused on the parliament. Ambassador William E. Kennard, a recent Obama appointee, was among those testifying at Monday's hearing, emphasizing the history of U.S.-European cooperation and shared values.

Nevertheless, he said, "while we share the same values, we implement them in different ways."

Kennard said the United States would oppose any attempt to make the new agreement invalidate the dozens of agreements, most of them secret, that the United States has with individual European governments. But several European Parliament members said leaving those accords intact would make no sense if they violate the pan-European agreement, insisting they would have to be updated.

"We will not be easy to deal with," one of them told Kennard.

"I would like to say this is just a bump in the road," the counterterrorism official in Washington said, speaking on the condition of anonymity because of the sensitivity of the subject. "But if the negotiating mandate contains some constraints on the commission that would eviscerate the agreement, then we're obviously concerned."

European privacy advocates have also raised objections to U.S. "data fishing," or combing through data to shake out suspects without a cause for suspicion; U.S. attempts to use passenger data to create profiles of likely terrorists; and data sharing among U.S. agencies, some of which might have nothing to do with counterterrorism.

"The whole collection of data, it's getting to a point where it's almost hysterical," in 't Veld said.

Parliament members expressed concern Monday about the lack of a reliable legal channel for Europeans to challenge what U.S. government agencies do with, and conclude from, data collected on them. U.S. citizens have such a right under the 1974 Privacy Act, but it excludes non-Americans.

Along with the specific objections, however, ran a current of irritation that Europeans are being asked to cooperate in a U.S. anti-terrorism campaign that many of them say has more than once veered off course - leading to torture, black prisons, extraordinary rendition and Guantanamo.

"Rather than the Americans dragging the European standards down, we should insist that the Americans live up to their own decent standards," said Douwe Korff of London Metropolitan University.

The undercurrent of irritation swelled in January when the United States began requiring U.S.-bound travelers from countries covered by a visa waiver program to register first with the **Department of Homeland Security**. Failure to register on a U.S. Web site at least two days before a flight can result in an airline refusing to allow a passenger to board, a prospect that limits last-minute travel.

The irritation was compounded by a recent announcement that as of last month, European travelers would be charged \$14 to register. Some European officials have described the registration and fee system as a visa by another name and threatened to impose a visa requirement on U.S. travelers to Europe in retaliation.

© 2010 The Washington Post Company

[Back To Table Of Contents](#)

UNCLASSIFIED

32. Chavez orders takeover of Owens-Illinois branch

Ian James, Associated Press, FederalNewsRadio.com, 26 October 2010

CARACAS, Venezuela (AP) -- Venezuelan President Hugo Chavez ordered the expropriation of U.S.-based glass container manufacturer Owens-Illinois Inc.'s subsidiary in the South American country.

Company spokeswoman Stephanie Johnston said Tuesday that "we were surprised to learn of this decision and we are prepared to work with government officials to better understand the situation."

Chavez announced plans to expropriate the company in a televised speech late Monday. The leftist leader criticized the company's practices in the country, saying it had been "taking away the money of Venezuelans" and exploiting local people.

Chavez did not detail his complaints about the Owens-Illinois, which is based in Perrysburg, Ohio.

"O-I has been supplying glass food and beverage containers to meet the needs of the Venezuelan people for more than 50 years," Johnston said. "Our two plants in Venezuela, located in Los Guayos and Valera, employ more than 1,000 people and represent less than 5 percent of our global segment operating profit."

Owens-Illinois is the world's largest glass container manufacturer, with operations in 22 countries.

The subsidiary Owens-Illinois de Venezuela CA counts among its clients Nestle, PepsiCo Inc. and Empresas Polar, which produces the local beer Polar. It was unclear how the takeover would affect supply agreements with the company's clients.

Earlier this year, Chavez threatened to "go after" Empresas Polar, the country's biggest food producer, while calling it a monopoly and accusing it of evading government price controls on basic foodstuffs by producing fewer of price-controlled items. Polar has denied wrongdoing.

At Owens-Illinois' plant in Los Guayos, union leader Rigoberto Mendez said "we don't have any reason to doubt that this expropriation is aimed at affecting the operations of Polar, a business that purchases 80 percent of our production."

Employees were working normally at the plant but are concerned, Mendez said in an interview by telephone.

"Our jobs are threatened, our salaries," Mendez said, insisting there are no labor conflicts at the company and that a government takeover would hurt a successful business.

It was unclear how soon the expropriation could take effect, or how Chavez's government would handle compensation for Owens-Illinois' assets.

In Washington, U.S. State Department spokesman Charles Luoma-Overstreet said: "We would expect Venezuela to provide prompt, adequate, and effective compensation for any expropriation of the investments of Owens-Illinois in accordance with international law."

Chavez has nationalized or expropriated a wide range of companies, including cement makers, retail stores and a steel maker, while seeking to lead Venezuela toward a socialist system.

Government opponents and business leaders say the seizures are hobbling the economy and spooking investors.

Chavez said in his speech that more expropriations are planned.

"There's another list around here," Chavez said, but added that he would save additional announcements for later.

Associated Press writers Jorge Rueda in Caracas and Luis Alonso Lugo in Washington contributed to this report.

Copyright 2010 The Associated Press. All rights reserved.

[Back To Table Of Contents](#)

UNCLASSIFIED

33. William Broe, former high-level CIA official, dies at 97

T. Rees Shapiro, Washington Post, 26 October 2010

William V. Broe, 97, a CIA officer who rose to become chief of operations in the Western Hemisphere and oversaw the agency's covert missions to destabilize the government of Salvador Allende, Chile's Marxist president, died of congestive heart failure Sept. 28 at a nursing home in Hingham, Mass. He was a resident of North Scituate, Mass.

Mr. Broe was an FBI special agent before joining the fledgling CIA in 1948. He held many assignments in the Far East as he worked his way up the organizational ranks. He was station chief in Tokyo before becoming chief of the Western Hemisphere division in 1965.

He held that job for seven years, during which time the division conducted clandestine operations in South America. Many of its efforts were a response to government concerns about the possible spread of communism and Soviet influence.

In March 1973, Mr. Broe made headlines after his "unprecedented" appearance before Senate investigators looking into CIA activities in South America. Specifically, the investigators were interested in the agency's alleged collaboration with International Telephone and Telegraph to interfere in Chilean political affairs.

ITT had worked actively against Allende's election in 1970, spending hundreds of thousands of dollars to fund political opposition. Once Allende was in power, the conglomerate feared its business interests in Chile would be nationalized.

Mr. Broe's testimony marked the first time an active clandestine agent of the CIA spoke on the record for a Senate investigation.

In his testimony, Mr. Broe said that he had met multiple times with ITT Chief Executive Harold Geneen and Senior Vice President Edward Gerrity under direct orders from CIA Director Richard Helms.

Mr. Broe, Geneen and Gerrity discussed employing a coordinated plan between the telecommunications conglomerate and the spy agency to create fiscal instability in Chile.

"There was a thesis," Mr. Broe told the Senate investigators, "that additional deterioration in the economic situation could influence a large number" of voters to push Allende out of office.

The ITT executives also offered to provide the CIA with funding to support an Allende presidential opponent, but Mr. Broe reportedly turned them down.

Peter Kornbluh, senior analyst at the National Security Archive at George Washington University and author of a 2003 book on Chile called "The Pinochet File," said in an interview that Mr. Broe was deeply "involved in operations to thwart" Allende's presidency.

Kornbluh said the CIA's connection and collaboration with ITT was one of the spy agency's biggest blunders because it set in motion the use of corporate money to fund covert U.S. foreign policy.

President Nixon - whose blunt instructions to the CIA on the Chilean situation were to "make the economy scream," according to multiple sources - authorized a number of crippling economic sanctions against the South American country.

The CIA spent millions in Chile on clandestine activities to sow dissension against Allende, including covert funding to one of Chile's widely read newspapers, El Mercurio, to plant stories and propaganda.

After Mr. Broe left his position as Western Hemisphere chief, and after his testimony on ITT, a bloody military coup in late 1973 toppled Allende and installed Gen. Augusto Pinochet in power.

Allende reportedly killed himself instead of surrendering to the military, which had assaulted the presidential palace in an air and ground attack.

In addition to his work in Chile, Mr. Broe also kept his eye on Fidel Castro's Cuba. Kornbluh said one of Mr. Broe's "biggest victories on the Cuban revolution" was the CIA-assisted effort to track down and execute Marxist revolutionary Ernesto "Che" Guevara in Bolivia in 1967.

Mr. Broe spent his last year at the CIA as inspector general and helped prepare and review documents during the Watergate investigation. He retired in 1973.

Mr. Broe was never charged with any wrongdoing for his CIA work. Helms, who also was a witness before the Senate committee, was convicted of perjury for failing to testify fully about the CIA's covert role in Chile. Helms was fined \$2,000 and received a suspended two-year prison sentence.

William Vincent Broe was born Aug. 24, 1913, in Amesbury, Mass. He was a 1939 biology and chemistry graduate of Bowdoin College in Maine. In 1942, he joined the FBI, where he specialized in counterintelligence.

In retirement, Mr. Broe served as a treasurer of his church in Cohasset, Mass., and planted roses in his garden.

His wife of 45 years, Jean Causer Broe, died in 1988. Survivors include four daughters, Barbara Burk of Marshall, Va., Kristine Broe of North Scituate, Susan Parmelee of Solon, Ohio, and Bonnie Broe of Scituate Harbor, Mass.; five grandchildren; and three great-grandchildren.

© 2010 The Washington Post Company

[Back To Table Of Contents](#)

34. The Online Threat

Should we be worried about a cyber war?

Seymour M. Hersh, The New Yorker, 1 November 2010

On April 1, 2001, an American EP-3E Aries II reconnaissance plane on an eavesdropping mission collided with a Chinese interceptor jet over the South China Sea, triggering the first international crisis of George W. Bush's Administration. The Chinese jet crashed, and its pilot was killed, but the pilot of the American aircraft, Navy Lieutenant Shane Osborn, managed to make an emergency landing at a Chinese F-8 fighter base on Hainan Island, fifteen miles from the mainland. Osborn later published a memoir, in which he described the "incessant jackhammer vibration" as the plane fell eight thousand feet in thirty seconds, before he regained control.

The plane carried twenty-four officers and enlisted men and women attached to the Naval Security Group Command, a field component of the National Security Agency. They were repatriated after eleven days; the plane stayed behind. The Pentagon told the press that the crew had followed its protocol, which called for the use of a fire axe, and even hot coffee, to disable the plane's equipment and software. These included an operating system created and controlled by the N.S.A., and the drivers needed to monitor encrypted Chinese radar, voice, and electronic communications. It was more than two years before the Navy acknowledged that things had not gone so well. "Compromise by the People's Republic of China of undestroyed classified material . . . is highly probable and cannot be ruled out," a Navy report issued in September, 2003, said.

The loss was even more devastating than the 2003 report suggested, and its dimensions have still not been fully revealed. Retired Rear Admiral Eric McVadon, who flew patrols off the coast of Russia and served as a defense attaché in Beijing, told me that the radio reports from the aircraft indicated that essential electronic gear had been dealt with. He said that the crew of the EP-3E managed to erase the hard drive—"zeroed it out"—but did not destroy the hardware, which left data retrievable: "No one took a hammer." Worse, the electronics had recently been upgraded. "Some might think it would not turn out as badly as it did, but I sat in some meetings about the intelligence cost," McVadon said. "It was grim."

The Navy's experts didn't believe that China was capable of reverse-engineering the plane's N.S.A.-supplied operating system, estimated at between thirty and fifty million lines of computer code, according to a former senior intelligence official. Mastering it would give China a road map for decrypting the Navy's classified intelligence and operational data. "If the operating system was controlling what you'd expect on an

intelligence aircraft, it would have a bunch of drivers to capture radar and telemetry," Whitfield Diffie, a pioneer in the field of encryption, said. "The plane was configured for what it wants to snoop, and the Chinese would want to know what we wanted to know about them-what we could intercept and they could not." And over the next few years the U.S. intelligence community began to "read the tells" that China had access to sensitive traffic.

The U.S. realized the extent of its exposure only in late 2008. A few weeks after Barack Obama's election, the Chinese began flooding a group of communications links known to be monitored by the N.S.A. with a barrage of intercepts, two Bush Administration national-security officials and the former senior **intelligence official** told me. The intercepts included details of planned American naval movements. The Chinese were apparently showing the U.S. their hand. ("The N.S.A. would ask, 'Can the Chinese be that good?' " the former official told me. "My response was that they only invented gunpowder in the tenth century and built the bomb in 1965. I'd say, 'Can you read Chinese?' We don't even know the Chinese pictograph for 'Happy hour.' ")

Why would the Chinese reveal that they had access to American communications? One of the Bush national-security officials told me that some of the aides then working for Vice-President Dick Cheney believed-or wanted to believe-that the barrage was meant as a welcome to President Obama. It is also possible that the Chinese simply made a mistake, given the difficulty of operating surgically in the cyber world.

Admiral Timothy J. Keating, who was then the head of the Pacific Command, convened a series of frantic meetings in Hawaii, according to a former **C.I.A.** official. In early 2009, Keating brought the issue to the new Obama Administration. If China had reverse-engineered the EP-3E's operating system, all such systems in the Navy would have to be replaced, at a cost of hundreds of millions of dollars. After much discussion, several current and former officials said, this was done. (The Navy did not respond to a request for comment on the incident.)

Admiral McVadon said that the loss prompted some black humor, with one Navy program officer quoted as saying, "This is one hell of a way to go about getting a new operating system."

The EP-3E debacle fuelled a longstanding debate within the military and in the Obama Administration. Many military leaders view the Chinese penetration as a warning about present and future vulnerabilities-about the possibility that China, or some other nation, could use its expanding cyber skills to attack America's civilian infrastructure and military complex. On the other side are those who argue for a civilian response to the threat, focussed on a wider use of encryption. They fear that an overreliance on the military will have adverse consequences for privacy and civil liberties.

In May, after years of planning, the U.S. Cyber Command was officially activated, and took operational control of disparate cyber-security and attack units that had been scattered among the four military services. Its commander, Army General Keith Alexander, a career intelligence officer, has made it clear that he wants more access to e-mail, social networks, and the Internet to protect America and fight in what he sees as a new warfare domain-cyberspace. In the next few months, President Obama, who has publicly pledged that his Administration will protect openness and privacy on the Internet, will have to make choices that will have enormous consequences for the future of an ever-growing maze of new communication techniques: Will America's networks be entrusted to civilians or to the military? Will cyber security be treated as a kind of war?

Even as the full story of China's EP-3E coup remained hidden, "cyber war" was emerging as one of the nation's most widely publicized national-security concerns. Early this year, Richard Clarke, a former White House national-security aide who warned about the threat from Al Qaeda before the September 11th attacks, published "Cyber War," an edgy account of America's vulnerability to hackers, both state-sponsored and individual, especially from China. "Since the late 1990s, China has systematically done all the things a nation would do if it contemplated having an offensive cyber war capability," Clarke wrote. He forecast a world in which China might unleash havoc:

Within a quarter of an hour, 157 major metropolitan areas have been thrown into knots by a nationwide power blackout hitting during rush hour. Poison gas clouds are wafting toward Wilmington and Houston. Refineries are burning up oil supplies in several cities. Subways have crashed in New York, Oakland, Washington, and Los Angeles. . . . Aircraft are literally falling out of the sky as a result of midair collisions across the country. . . . Several thousand Americans have already died.

Retired Vice-Admiral J. Michael McConnell, Bush's second director of National Intelligence, has issued similar warnings. "The United States is fighting a cyber war today, and we are losing," McConnell wrote earlier this year in the Washington Post. "Our cyber-defenses are woefully lacking." In February, in testimony before the Senate Commerce, Science, and Transportation Committee, he said, "As a consequence of not mitigating the risk, we're going to have a catastrophic event."

A great deal of money is at stake. Cyber security is a major growth industry, and warnings from Clarke, McConnell, and others have helped to create what has become a military-cyber complex. The federal government currently spends between six and seven billion dollars annually for unclassified cyber-security work, and, it is estimated, an equal amount on the classified portion. In July, the Washington Post published a critical assessment of the unchecked growth of government intelligence agencies and private contractors. Benjamin Powell, who served as general counsel for three directors of the Office of National Intelligence, was quoted as saying of the cyber-security sector, "Sometimes there was an unfortunate attitude of bring your knives, your guns, your fists, and be fully prepared to defend your turf. . . . Because it's funded, it's hot and it's sexy."

Clarke is the chairman of Good Harbor Consulting, a strategic-planning firm that advises governments and companies on cyber security and other issues. (He says that more than ninety per cent of his company's revenue comes from non-cyber-related work.) McConnell is now an executive vice-president of Booz Allen Hamilton, a major defense contractor. Two months after McConnell testified before the Senate, Booz Allen Hamilton landed a thirty-four-million-dollar cyber contract. It included fourteen million dollars to build a bunker for the Pentagon's new Cyber Command.

American intelligence and security officials for the most part agree that the Chinese military, or, for that matter, an independent hacker, is theoretically capable of creating a degree of chaos inside America. But I was told by military, technical, and intelligence experts that these

fears have been exaggerated, and are based on a fundamental confusion between cyber espionage and cyber war. Cyber espionage is the science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence. Cyber war involves the penetration of foreign networks for the purpose of disrupting or dismantling those networks, and making them inoperable. (Some of those I spoke to made the point that China had demonstrated its mastery of cyber espionage in the EP-3E incident, but it did not make overt use of it to wage cyber war.) Blurring the distinction between cyber war and cyber espionage has been profitable for defense contractors-and dispiriting for privacy advocates.

Clarke's book, with its alarming vignettes, was praised by many reviewers. But it received much harsher treatment from writers in the technical press, who pointed out factual errors and faulty assumptions. For example, Clarke attributed a severe power outage in Brazil to a hacker; the evidence pointed to sooty insulators.

The most common cyber-war scare scenarios involve America's electrical grid. Even the most vigorous privacy advocate would not dispute the need to improve the safety of the power infrastructure, but there is no documented case of an electrical shutdown forced by a cyber attack. And the cartoonish view that a hacker pressing a button could cause the lights to go out across the country is simply wrong. There is no national power grid in the United States. There are more than a hundred publicly and privately owned power companies that operate their own lines, with separate computer systems and separate security arrangements. The companies have formed many regional grids, which means that an electrical supplier that found itself under cyber attack would be able to avail itself of power from nearby systems. Decentralization, which alarms security experts like Clarke and many in the military, can also protect networks.

In July, there were reports that a computer worm, known as Stuxnet, had infected thousands of computers worldwide. Victims, most of whom were unharmed, were able to overcome the attacks, although it sometimes took hours or days to even notice them. Some of the computers were inside the Bushehr nuclear-energy plant, in Iran, and this led to speculation that Israel or the United States might have developed the virus. A Pentagon adviser on information warfare told me that it could have been an attempted "semantic attack," in which the virus or worm is designed to fool its victim into thinking that its computer systems are functioning properly, when in fact they are not, and may not have been for some time. (This month, Microsoft, whose Windows operating systems were the main target of Stuxnet, completed a lengthy security fix, or patch.)

If Stuxnet was aimed specifically at Bushehr, it exhibited one of the weaknesses of cyber attacks: they are difficult to target and also to contain. India and China were both hit harder than Iran, and the virus could easily have spread in a different direction, and hit Israel itself. Again, the very openness of the Internet serves as a deterrent against the use of cyber weapons.

Bruce Schneier, a computer scientist who publishes a widely read blog on cyber security, told me that he didn't know whether Stuxnet posed a new threat. "There's certainly no actual evidence that the worm is targeted against Iran or anybody," he said in an e-mail. "On the other hand, it's very well designed and well written." The real hazard of Stuxnet, he added, might be that it was "great for those who want to believe cyber war is here. It is going to be harder than ever to hold off the military."

A defense contractor who is regarded as one of America's most knowledgeable experts on Chinese military and cyber capabilities took exception to the phrase "cyber war." "Yes, the Chinese would love to stick it to us," the contractor told me. "They would love to transfer economic and business innovation from West to East. But cyber espionage is not cyber war." He added, "People have been sloppy in their language. McConnell and Clarke have been pushing cyber war, but their evidentiary basis is weak."

James Lewis, a senior fellow at the Center for Strategic and International Studies, who worked for the Departments of State and Commerce in the Clinton Administration, has written extensively on the huge economic costs due to cyber espionage from China and other countries, like Russia, whose hackers are closely linked to organized crime. Lewis, too, made a distinction between this and cyber war: "Current Chinese officials have told me that we're not going to attack Wall Street, because we basically own it"-a reference to China's holdings of nearly a trillion dollars in American securities-"and a cyber-war attack would do as much economic harm to us as to you."

Nonetheless, China "is in full economic attack" inside the United States, Lewis says. "Some of it is economic espionage that we know and understand. Some of it is like the Wild West. Everybody is pirating from everybody else. The U.S.'s problem is what to do about it. I believe we have to begin by thinking about it"-the Chinese cyber threat-"as a trade issue that we have not dealt with."

The bureaucratic battle between the military and civilian agencies over cyber security-and the budget that comes with it-has made threat assessments more problematic. General Alexander, the head of Cyber Command, is also the director of the N.S.A., a double role that has caused some apprehension, particularly on the part of privacy advocates and civil libertarians. (The N.S.A. is formally part of the Department of Defense.) One of Alexander's first goals was to make sure that the military would take the lead role in cyber security and in determining the future shape of computer networks. (A Department of Defense spokesman, in response to a request to comment on this story, said that the department "continues to adhere to all laws, policies, directives, or regulations regarding cyberspace. The Department of Defense maintains strong commitments to protecting civil liberties and privacy.")

The **Department of Homeland Security** has nominal responsibility for the safety of America's civilian and private infrastructure, but the military leadership believes that the D.H.S. does not have the resources to protect the electrical grids and other networks. (The department intends to hire a thousand more cyber-security staff members over the next three years.) This dispute became public when, in March, 2009, Rodney Beckstrom, the director of the D.H.S.'s National **Cybersecurity** Center, abruptly resigned. In a letter to Secretary **Janet Napolitano**, Beckstrom warned that the N.S.A. was effectively controlling her department's cyber operations: "While acknowledging the critical importance of N.S.A. to our intelligence efforts . . . the threats to our democratic processes are significant if all top level government network security and monitoring are handled by any one organization." Beckstrom added that he had argued for civilian control of cyber security, "which interfaces with, but is not controlled by, the N.S.A."

General Alexander has done little to reassure critics about the N.S.A.'s growing role. In the public portion of his confirmation hearing, in April, before the Senate Armed Services Committee, he complained of a "mismatch between our technical capabilities to conduct

operations and the governing laws and policies."

Alexander later addressed a controversial area: when to use conventional armed forces to respond to, or even preempt, a network attack. He told the senators that one problem for Cyber Command would be to formulate a response based on nothing more than a rough judgment about a hacker's intent. "What's his game plan? Does he have one?" he said. "These are tough issues, especially when attribution and neutrality are brought in, and when trying to figure out what's come in." At this point, he said, he did not have "the authority . . . to reach out into a neutral country and do an attack. And therein lies the complication. . . . What do you do to take that second step?"

Making the same argument, William J. Lynn III, the Deputy Secretary of Defense, published an essay this fall in *Foreign Affairs* in which he wrote of applying the N.S.A.'s "defense capabilities beyond the '.gov' domain," and asserted, "As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare." This definition raises questions about where the battlefield begins and where it ends. If the military is operating in "cyberspace," does that include civilian computers in American homes?

Lynn also alluded to a previously classified incident, in 2008, in which some N.S.A. unit commanders, facing penetration of their bases' secure networks, concluded that the break-in was caused by a disabling thumb drive; Lynn said that it had been corrupted by "a foreign intelligence agency." (According to press reports, the program was just as likely to be the product of hackers as that of a government.) Lynn termed it a "wake-up call" and a "turning point in U.S. cyber defense strategy." He compared the present moment to the day in 1939 when President Franklin D. Roosevelt got a letter from Albert Einstein about the possibility of atomic warfare.

But Lynn didn't mention one key element in the commanders' response: they ordered all ports on the computers on their bases to be sealed with liquid cement. Such a demand would be a tough sell in the civilian realm. (And a Pentagon adviser suggested that many military computer operators had simply ignored the order.)

A senior official in the **Department of Homeland Security** told me, "Every time the N.S.A. gets involved in domestic security, there's a hue and cry from people in the privacy world." He said, though, that cooperation between the military and civilians had increased. (The **Department of Homeland Security** recently signed a memorandum with the Pentagon that gives the military authority to operate inside the United States in case of cyber attack.) "We need the N.S.A., but the question we have is how to work with them and still say and demonstrate that we are in charge in the areas for which we are responsible."

This official, like many I spoke to, portrayed the talk about cyber war as a bureaucratic effort "to raise the alarm" and garner support for an increased Defense Department role in the protection of private infrastructure. He said, "You hear about cyber war all over town. This"-he mentioned statements by Clarke and others-"is being done to mobilize a political effort. We always turn to war analogies to mobilize the people."

In theory, the fight over whether the Pentagon or civilian agencies should be in charge of cyber security should be mediated by President Obama's coordinator for cyber security, Howard Schmidt-the cyber czar. But Schmidt has done little to assert his authority. He has no independent budget control and in a crisis would be at the mercy of those with more assets, such as General Alexander. He was not the Administration's first choice for the cyber-czar job-reportedly, several people turned it down. The Pentagon adviser on information warfare, in an e-mail that described the lack of an over-all policy and the "cyber-pillage" of intellectual property, added the sort of dismissive comment that I heard from others: "It's ironic that all this goes on under the nose of our first cyber President. . . . Maybe he should have picked a cyber czar with more than a mail-order degree." (Schmidt's bachelor's and master's degrees are from the University of Phoenix.)

Howard Schmidt doesn't like the term "cyber war." "The key point is that cyber war benefits no one," Schmidt told me in an interview at the Old Executive Office Building. "We need to focus on that fact. When people tell me that these guys or this government is going to take down the U.S. military with information warfare I say that, if you look at the history of conflicts, there's always been the goal of intercepting the communications of combatants-whether it's cutting down telephone poles or intercepting Morse-code signalling. We have people now who have found that warning about 'cyber war' has become an unlikely career path"-an obvious reference to McConnell and Clarke. "All of a sudden, they have become experts, and they get a lot of attention. 'War' is a big word, and the media is responsible for pushing this, too. Economic espionage on the Internet has been mischaracterized by people as cyber war."

Schmidt served in Vietnam, worked as a police officer for several years on a SWAT team in Arizona, and then specialized in computer-related crimes at the F.B.I. and in the Air Force's investigative division. In 1997, he joined Microsoft, where he became chief of security, leaving after the 9/11 attacks to serve in the Bush Administration as a special adviser for cyber security. When Obama hired him, he was working as the head of security for eBay. When I asked him about the ongoing military-civilian dispute, Schmidt said, "The middle way is not to give too much authority to one group or another and to make sure that we share information with each other."

Schmidt continued, "We have to protect our infrastructure and our way of life, for sure. We do have vulnerabilities, and we do talk about worst-case scenarios" with the Pentagon and the **Department of Homeland Security**. "You don't see a looming war and just wait for it to come." But, at the same time, "we have to keep our shipping lanes open, to continue to do commerce, and to freely use the Internet."

How should the power grid be protected? It does remain far too easy for a sophisticated hacker to break into American networks. In 2008, the computers of both the Obama and the McCain campaigns were hacked. Suspicion fell on Chinese hackers. People routinely open e-mails with infected attachments, allowing hackers to "enslave" their computers. Such machines, known as zombies, can be linked to create a "botnet," which can flood and effectively shut down a major system. Hackers are also capable of penetrating a major server, like Gmail. Guesses about the cost of cyber crime vary widely, but one survey, cited by President Obama in a speech in May, 2009, put the price at more than eight billion dollars in 2007 and 2008 combined. Obama added, referring to corporate cyber espionage, "It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to one trillion dollars."

One solution is mandated encryption: the government would compel both corporations and individuals to install the most up-to-date

protection tools. This option, in some form, has broad support in the technology community and among privacy advocates. In contrast, military and intelligence eavesdroppers have resisted nationwide encryption since 1976, when the Diffie-Hellman key exchange (an encryption tool co-developed by Whitfield Diffie) was invented, for the most obvious of reasons: it would hinder their ability to intercept signals. In this sense, the N.S.A.'s interests align with those of the hackers.

John Arquilla, who has taught since 1993 at the U.S. Naval Postgraduate School in Monterey, California, writes in his book "Worst Enemies," "We would all be far better off if virtually all civil, commercial, governmental, and military internet and web traffic were strongly encrypted." Instead, many of those charged with security have adopted the view that "cyberspace can be defended with virtual fortifications-basically the 'firewalls' that everyone knows about. . . . A kind of Maginot Line mentality prevails."

Arquilla added that America's intelligence agencies and law-enforcement officials have consistently resisted encryption because of fears that a serious, widespread effort to secure data would interfere with their ability to electronically monitor and track would-be criminals or international terrorists. This hasn't stopped sophisticated wrongdoers from, say, hiring hackers or encrypting files; it just leaves the public exposed, Arquilla writes. "Today drug lords still enjoy secure internet and web communications, as do many in terror networks, while most Americans don't."

Schmidt told me that he supports mandated encryption for the nation's power and electrical infrastructure, though not beyond that. But, early last year, President Obama declined to support such a mandate, in part, Schmidt said, because of the costs it would entail for corporations. In addition to the setup expenses, sophisticated encryption systems involve a reliance on security cards and on constantly changing passwords, along with increased demands on employees and a ceding of control by executives to their security teams.

General Alexander, meanwhile, has continued to press for more authority, and even for a separate Internet domain-another Maginot Line, perhaps. One morning in September, he told a group of journalists that the Cyber Command needed what he called "a secure zone," a separate space within the Internet to shelter the military and essential industries from cyber attacks. The secure zone would be kept under tight government control. He also assured the journalists, according to the *Times*, that "we can protect civil liberties, privacy, and still do our mission." The General was more skeptical about his ability to please privacy advocates when he testified, a few hours later, before the House Armed Services Committee: "A lot of people bring up privacy and civil liberties. And then you say, 'Well, what specifically are you concerned about?' And they say, 'Well, privacy and civil liberties.' . . . Are you concerned that the anti-virus program that McAfee runs invades your privacy or civil liberties?' And the answer is 'No, no, no-but I'm worried that you would.' "

This summer, the *Wall Street Journal* reported that the N.S.A. had begun financing a secret surveillance program called Perfect Citizen to monitor attempted intrusions into the computer networks of private power companies. The program calls for the installation of government sensors in those networks to watch for unusual activity. The Journal noted that some companies expressed concerns about privacy, and said that what they needed instead was better guidance on what to do in case of a major cyber attack. The N.S.A. issued a rare public response, insisting that there was no "monitoring activity" involved: "We strictly adhere to both the spirit and the letter of U.S. laws and regulations."

A former N.S.A. operative I spoke to said, of Perfect Citizen, "This would put the N.S.A. into the job of being able to watch over our national communications grid. If it was all dot-gov, I would have no problem with the sensors, but what if the private companies rely on Gmail or att.net to communicate? This could put the N.S.A. into every service provider in the country."

The N.S.A. has its own hackers. Many of them are based at a secret annex near Thurgood Marshall International Airport, outside Baltimore. (The airport used to be called Friendship Airport, and the annex is known to insiders as the FANX, for "Friendship annex.") There teams of attackers seek to penetrate the communications of both friendly and unfriendly governments, and teams of defenders monitor penetrations and attempted penetrations of U.S. systems. The former N.S.A. operative, who served as a senior watch officer at a major covert installation, told me that the N.S.A. obtained invaluable on-the-job training in cyber espionage during the attack on Iraq in 1991. Its techniques were perfected during the struggle in Kosovo in 1999 and, later, against Al Qaeda in Iraq. "Whatever the Chinese can do to us, we can do better," the technician said. "Our offensive cyber capabilities are far more advanced."

Nonetheless, Marc Rotenberg, the president of the Electronic Privacy Information Center and a leading privacy advocate, argues that the N.S.A. is simply not competent enough to take a leadership role in cyber security. "Let's put the issue of privacy of communications aside," Rotenberg, a former Senate aide who has testified often before Congress on encryption policy and consumer protection, said. "The question is: Do you want an agency that spies with mixed success to be responsible for securing the nation's security? If you do, that's crazy."

Nearly two decades ago, the Clinton Administration, under pressure from the N.S.A., said that it would permit encryption-equipped computers to be exported only if their American manufacturers agreed to install a government-approved chip, known as the Clipper Chip, in each one. It was subsequently revealed that the Clipper Chip would enable law-enforcement officials to have access to data in the computers. The ensuing privacy row embarrassed Clinton, and the encryption-equipped computers were permitted to be exported without the chip, in what amounted to a rebuke to the N.S.A.

That history may be repeating itself. The Obama Administration is now planning to seek broad new legislation that would enable national-security and law-enforcement officials to police online communications. The legislation, similar to that sought two decades ago in the Clipper Chip debate, would require manufacturers of equipment such as the BlackBerry, and all domestic and foreign purveyors of communications, such as Skype, to develop technology that would allow the federal government to intercept and decode traffic.

"The lesson of Clipper is that the N.S.A. is really not good at what it does, and its desire to eavesdrop overwhelms its ability to protect, and puts at risk U.S. security," Rotenberg said. "The N.S.A. wants security, sure, but it also wants to get to capture as much as it can. Its view is you can get great security as long as you listen in." Rotenberg added, "General Alexander is not interested in communication privacy. He's not pushing for encryption. He wants to learn more about people who are on the Internet"-to get access to the original internal protocol, or

I.P., addresses identifying the computers sending e-mail messages. "Alexander wants user I.D. He wants to know who you are talking to."

Rotenberg concedes that the government has a role to play in the cyber world. "We privacy guys want strong encryption for the security of America's infrastructure," he said. He also supports Howard Schmidt in his willingness to mandate encryption for the few industries whose disruption could lead to chaos. "Howard is trying to provide a reasoned debate on an important issue."

Whitfield Diffie, the encryption pioneer, offered a different note of skepticism in an e-mail to me: "It would be easy to write a rule mandating encryption but hard to do it in such a way as to get good results. To make encryption effective, someone has to manage and maintain the systems (the way N.S.A. does for D.O.D. and, to a lesser extent, other parts of government). I think that what is needed is more by way of standards, guidance, etc., that would make it easier for industry to implement encryption without making more trouble for itself than it saves."

More broadly, Diffie wrote, "I am not convinced that lack of encryption is the primary problem. The problem with the Internet is that it is meant for communications among non-friends."

What about China? Does it pose such a threat that, on its own, it justifies putting cyber security on a war footing? The U.S. has long viewed China as a strategic military threat, and as a potential adversary in the sixty-year dispute over Taiwan. Contingency plans dating back to the Cold War include calls for an American military response, led by a Navy carrier group, if a Chinese fleet sails into the Taiwan Strait. "They'll want to stop our carriers from coming, and they will throw whatever they have in cyber war-everything but the kitchen sink-to blind us, or slow our fleet down," Admiral McVadon, the retired defense attaché, said. "Our fear is that the Chinese may think that cyber war will work, but it may not. And that's a danger because it"-a test of cyber warfare-"could lead to a bigger war."

However, the prospect of a naval battle for Taiwan and its escalation into a cyber attack on America's domestic infrastructure is remote. Jonathan Pollack, an expert on the Chinese military who teaches at the Naval War College in Newport, Rhode Island, said, "The fact is that the Chinese are remarkably risk-averse." He went on, "Yes, there have been dustups, and the United States collects intelligence around China's border, but there is an accommodation process under way today between China and Taiwan." In June, Taiwan approved a trade agreement with China that had, as its ultimate goal, a political rapprochement. "The movement there is palpable, and, given that, somebody's got to tell me how we are going to find ourselves in a war with China," Pollack said.

Many long-standing allies of the United States have been deeply engaged in cyber espionage for decades. A retired four-star Navy admiral, who spent much of his career in signals intelligence, said that Russia, France, Israel, and Taiwan conduct the most cyber espionage against the U.S. "I've looked at the extraordinary amount of Russian and Chinese cyber activity," he told me, "and I am hard put to it to sort out how much is planning for warfare and how much is for economic purposes."

The admiral said that the U.S. Navy, worried about budget cuts, "needs an enemy, and it's settled on China," and that "using what your enemy is building to justify your budget is not a new game."

There is surprising unanimity among cyber-security experts on one issue: that the immediate cyber threat does not come from traditional terrorist groups like Al Qaeda, at least, not for the moment. "Terrorist groups are not particularly good now in attacking our computer system," John Arquilla told me. "They're not that interested in it-yet. The question is: Do vulnerabilities exist inside America? And, if they do, the terrorists eventually will exploit them." Arquilla added a disturbing thought: "The terrorists of today rely on cyberspace, and they have to be good at cyber security to protect *their* operations." As terrorist groups get better at defense, they may eventually turn to offense.

Jeffrey Carr, a Seattle-based consultant on cyber issues, looked into state and non-state cyber espionage throughout the recent conflicts in Estonia and Georgia. Carr, too, said he was skeptical that China or Russia would mount a cyber-war attack against the United States. "It's not in their interest to hurt the country that is feeding them money," he said. "On the other hand, it does make sense for lawless groups." He envisaged "five- or six-year-old kids in the Middle East who are working on the Internet," and who would "become radicalized fifteen- or sixteen-year-old hackers." Carr is an advocate of making all Internet service providers require their customers to use verifiable registration information, as a means of helping authorities reduce cyber espionage.

Earlier this year, Carr published "Inside Cyber Warfare," an account, in part, of his research into cyber activity around the world. But he added, "I hate the term 'cyber war.'" Asked why he used "cyber warfare" in the title of his book, he responded, "I don't like hype, but hype sells."

Why not ignore the privacy community and put cyber security on a war footing? Granting the military more access to private Internet communications, and to the Internet itself, may seem prudent to many in these days of international terrorism and growing American tensions with the Muslim world. But there are always unintended consequences of military activity-some that may take years to unravel. Ironically, the story of the EP-3E aircraft that was downed off the coast of China provides an example. The account, as relayed to me by a fully informed retired American diplomat, begins with the contested Presidential election between Vice-President Al Gore and George W. Bush the previous November. That fall, a routine military review concluded that certain reconnaissance flights off the eastern coast of the former Soviet Union-daily Air Force and Navy sorties flying out of bases in the Aleutian Islands-were redundant, and recommended that they be cut back.

"Finally, on the eve of the 2000 election, the flights were released," the former diplomat related. "But there was nobody around with any authority to make changes, and everyone was looking for a job." The reality is that no military commander would unilaterally give up any mission. "So the system defaulted to the next target, which was China, and the surveillance flights there went from one every two weeks or so to something like one a day," the former diplomat continued. By early December, "the Chinese were acting aggressively toward our now increased reconnaissance flights, and we complained to our military about their complaints. But there was no one with political authority in Washington to respond, or explain." The Chinese would not have been told that the increase in American reconnaissance had little to do

with anything other than the fact that inertia was driving day-to-day policy. There was no leadership in the Defense Department, as both Democrats and Republicans waited for the Supreme Court to decide the fate of the Presidency.

The predictable result was an increase in provocative behavior by Chinese fighter pilots who were assigned to monitor and shadow the reconnaissance flights. This evolved into a pattern of harassment in which a Chinese jet would maneuver a few dozen yards in front of the slow, plodding EP-3E, and suddenly blast on its afterburners, soaring away and leaving behind a shock wave that severely rocked the American aircraft. On April 1, 2001, the Chinese pilot miscalculated the distance between his plane and the American aircraft. It was a mistake with consequences for the American debate on cyber security that have yet to be fully reckoned.

The New Yorker © 2010 Condé Nast Digital. All rights reserved.

[Back To Table Of Contents](#)

35. The Demographic Future

What Population Growth – and Decline – Means for the Global Economy
Nicholas Eberstadt, Foreign Affairs, November/December 2010

It is already possible to draw a reasonably reliable profile of the world's population in 2030. This is, of course, because the overwhelming majority of those who will inhabit the world 20 years from now are already alive. As a result, one can make some fairly confident estimates of important demographic trends, including manpower availability, the growth in the number of senior citizens, and the resulting support burden on workers.

Overall, it is apparent that the future global economy will not be able to rely on the kind of demographic inputs that helped fuel growth in the era before the current global recession. For today's affluent Western economies, the coming demographic challenge of stagnant and aging populations combined with mounting health and pension claims on a shrinking pool of prospective workers is already generating concern, especially in Europe and Japan. But at the same time, demographic constraints in the rising economies that are expected to fuel future global growth are more serious and intractable than generally recognized.

When the current painful and protracted economic crisis is eventually resolved, the global economy will likely embark again on a path of sustained long-term growth – but at a slower pace, because of new demographic realities. These demographic pressures can be substantially offset only if both rich and poor countries undertake profound and far-reaching changes in working arrangements, lifestyles, business practices, and government policies.

MORE HEALTH, FEWER BABIES

The twentieth century was an era of unprecedented population growth. Between 1900 and 2000, the world's population almost quadrupled, from about 1.6 billion people to around 6.1 billion. This huge expansion did not occur because people suddenly began reproducing at higher rates; instead, population surged because humans finally stopped dying like flies. Over the course of the twentieth century, global life expectancy at birth more than doubled, soaring from about 30 years in 1900 to about 65 years in 2000. This global population explosion was, in reality, a health explosion: the entirety of the enormous increase in human population over the past several generations was due to dramatic declines in mortality and improvements in general health conditions.

If the twentieth century's revolutionary demographic trend was a health explosion, the twenty-first century's hallmark trend appears to be a fertility implosion. A dramatic, far-reaching, and, as yet, unremitting global reduction in childbearing and birthrates is now under way. Sustained and deliberate reductions in family size through birth control began to lower national fertility levels in certain European countries long ago. But sustained fertility decline only became a worldwide phenomenon after the end of World War II. Over the past half century, according to the United Nations Population Division (UNDP) and the U.S. Census Bureau, the number of births per woman dropped by almost half, from 4.9 in the early 1960s to an estimated 2.5 today, with the steepest decline occurring in less developed countries.

Close to half of the world's population now lives in countries with fertility rates below the replacement level, which, as a rough rule of thumb, is 2.1 births per woman. In these states – absent steady compensatory immigration – current childbearing patterns will lead to an eventual and indefinite depopulation. Almost all of the world's developed countries have sub-replacement fertility, with overall birthrates more than 20 percent below the level required for long-term population stability. But developed countries account for less than a fifth of the world's population; the great majority of the world's populations with sub-replacement fertility in fact reside in low-income societies.

China is one such low-income society with sub-replacement fertility. It may seem exceptional, given Beijing's one-child policy. Yet sub-replacement fertility is also the norm today in many low-income countries without coercive population controls. Strikingly, some of these are countries with predominantly rural populations where educational opportunities for women remain limited and health conditions are still poor. One such case may be Myanmar (also called Burma), an impoverished and isolated country where, according to the UNDP, birth levels have fallen below the replacement rate.

The U.S. Census Bureau and the UNDP both estimate that sub-replacement fertility is the norm in every East Asian country and in much of Southeast Asia, including Vietnam and Thailand; in most of the Caribbean islands; and, increasingly, throughout Latin America. What is no less striking, sub-replacement fertility has also come to parts of the great Islamic expanse that stretches from northern Africa through the Middle East and into Asia.

Much remains unexplained about the continuing march toward ever-lower levels of fertility. For example, there are few socioeconomic preconditions for rapid and pronounced fertility decline or even for slides into sub-replacement fertility, as the case of Myanmar underscores. Furthermore, it is not known how long a society that has entered into sub-replacement-fertility mode will stay there: Japan, for example, began reporting sub-replacement fertility in the 1950s and has had uninterrupted sub-replacement fertility since the early 1970s. Demographers, it should be emphasized, still have no reliable techniques for making accurate long-term fertility forecasts. Nevertheless, some specialists argue that ultralow fertility rates may be but a harbinger of future – and currently unimaginable – fertility declines.

Although little is conclusively known about the underlying causes of the fertility revolution, some of its consequences are discernable. First, pronounced fertility declines today imply a slowdown in the growth of the working-age population tomorrow. Second, low fertility today leads to population aging tomorrow – a process that becomes turbocharged if sub-replacement birthrates are sustained over time.

MEN AT WORK

On a global level, returning to pre-crisis economic growth rates will be complicated by the impending – and inalterable – trends in worldwide manpower availability. Between now and 2030, the global supply of potential workers is set to grow much more slowly than in the previous two decades. According to U.S. Census Bureau projections, the absolute increase in the world's working-age (between 15 and 64) population between 2010 and 2030 will be around 900 million people, 400 million fewer than over the past two decades. The projected average rate of global manpower growth for the coming decades is 0.9 percent per year, only half the rate for the period between 1990 and 2010.

Complicating matters still further is the prospective regional distribution of the coming growth in global manpower. Over the past 20 years, the two greatest centers of manpower growth have been China and India, which also happened to be two of the world's most rapidly growing economies. Over the next 20 years, however, the largest share of growth in the world's working-age population – well over a third of the total – will take place in sub-Saharan Africa, the region with the worst record of long-term economic performance. Bangladesh and Pakistan will account for nearly another eighth of the world's manpower growth. In other words, over the next two decades, sub-Saharan Africa, Bangladesh, and Pakistan will generate nearly half the growth in the world's working-age population.

At the same time, most of the current advanced economies of the Organization for Economic Cooperation and Development (OECD) and many promising emerging economies are set to experience shrinkage in their working-age populations. This group includes China, Japan, the countries of eastern and western Europe, and the former Soviet states.

The prospect of shrinking manpower does not look any better when broken down into subsidiary age-group components. Younger workers are important for growth, because they typically have higher levels of education and better knowledge of the latest technology. But over the next 20 years, growth in the worldwide pool of young manpower will undergo a severe deceleration. According to U.S. Census Bureau projections, total young manpower – defined here as men and women between the ages of 15 and 29 – will increase by just four percent, or 70 million people, between today and 2030, representing barely a fifth of the increase over the past two decades. Only the countries of sub-Saharan Africa will see appreciable growth in young manpower. Japan and the states of western Europe are on course for significant prospective drops in this key manpower pool over the next 20 years (in the case of Japan, by almost 25 percent). But by far the most massive falloff in young manpower is set to take place in China: over the next 20 years, this working-age group will fall in China by around 100 million people, or about 30 percent.

Yet as young manpower grows relatively scarcer, older manpower is becoming increasingly abundant. Over the next 20 years, the oldest segment of the conventionally defined working-age population – men and women between 50 and 64 years of age – is projected to account for nearly half of all global manpower growth, nearly twice the share for the period between 1990 and 2010. China will face a particularly huge increase in older manpower; the working-age population will also age in many other emerging markets, as well as in all the developed Western economies. Older workers do bring some particular skills, based on experience, but they also tend to be less educated and less healthy than younger workers. Furthermore, labor-force participation rates for older workers tend to be lower, and in some affluent societies, much lower.

The prospective global work force of 2030 is on track to being more educated and healthier than previous generations of workers, which should increase overall labor productivity. But the economic potential of such prospective benefits should not be exaggerated. Projections by the International Institute for Applied Systems Analysis, in Austria, and the Vienna Institute of Demography suggest that improvements in educational levels for the world's working-age population stand to be slower over the next 20 years than they were over the past 20 years. For example, the proportion of global manpower with no education at all is projected to drop by less than five percentage points, compared to an eight-point drop in the past 20 years. And the share of the working-age population with secondary schooling or better is estimated to increase by ten points, three points fewer than in the previous two decades.

Taken as a whole, these manpower trends point to mounting demographic pressures – and, quite possibly, a slowdown in the rate of long-term economic growth. All other factors being equal, these trends also suggest a slowdown in consumer spending, which could perhaps lead to a slowdown in business profits, as well.

AGING UNGRACEFULLY?

The economic performance of the world's six major economies will largely determine growth patterns for the world as a whole over the next 20 years. China, India, Japan, Russia, western Europe, and the United States account for over half of the world's current population and over 70 percent of the world's GDP, adjusted for purchasing power parity. And over the decade before the current financial crisis, they accounted for about 70 percent of global economic growth.

No major economy has more radiant prospects for the coming decades than China. Its economic transformation has been nothing less than dazzling – according to World Bank estimates, in the three decades following Deng Xiaoping's 1978 moves toward systemic reform, China's GDP grew by almost ten percent a year. (Other sources suggest a slightly slower rate of growth but still one that is historically

unprecedented.) Beijing officially forecasts annual growth rates of roughly seven percent per year between now and 2030. But this rosy prognosis does not take into account China's looming demographic tempests. Population specialists believe that China became a sub-replacement-fertility society about two decades ago and that since then, birthrates have fallen far below the replacement level. For example, the U.S. Census Bureau puts China's total fertility rate at about 1.5 children per woman, or 30 percent below the level required for long-term population stability.

Persistent, and now extreme, sub-replacement fertility is the demographic driver shaping the China of tomorrow. Given current trends, U.S. Census Bureau projections anticipate fewer people under the age of 50 in China in 2030 than today and many fewer Chinese in their 20s and early 30s. These same projections foresee many more elderly Chinese in their 60s, 70s, and 80s. China's older workers are much less educated than their youthful successors – nearly half of today's working-age population between the ages of 50 and 64 has not completed primary school. Educational levels for older workers will improve in the decades ahead but will still lag behind Chinese national averages. And China will be experiencing a population explosion of senior citizens over the next 20 years; they are the progeny of the pre-population-control era. In 2010, about 115 million people in China were 65 or older. By 2030, this number is projected to approach 240 million people – meaning that China's cohort of senior citizens would be soaring at an average rate of 3.7 percent per year.

How Beijing will support this coming tsunami of senior citizens remains an unanswered question. As yet, China has no national public pension system and only the most rudimentary provisions for rural health care. Meeting the needs of its rapidly growing elderly population will place economic and social pressures on China that no country of a comparable income level has ever had to confront.

Moreover, in the decades ahead, China will face a growing number of young men who will never marry due to the country's one-child policy, which has resulted in a reported birth ratio of almost 120 boys for every 100 girls (most societies report the births of 103 to 105 boys for every 100 girls). This imbalance is setting the stage for a "marriage squeeze" of monumental proportions. By 2030, projections suggest that more than 25 percent of Chinese men in their late 30s will never have married. The coming marriage squeeze will likely be even more acute in the Chinese countryside, since the poor, uneducated, and rural population will be more likely to lose out in the competition for brides. Beijing will have to determine how it will cope with a growing demographic of unmarried, underprivileged, and, quite possibly, deeply discontented young men.

China still has potential sources for enhancing productivity, including the migration of rural workers to more productive urban jobs, the wider application of currently underutilized technical know-how, improved financial intermediation for the country's high savings rates, and broader institutional and policy reforms to enhance efficiency. Such untapped potential can fuel future growth, but nevertheless, China's serious demographic challenges could slow economic growth more than is currently expected.

Russia is another emerging-market country widely regarded as holding immense economic promise, not least by the leaders in the Kremlin. Despite the current economic downturn, official Russian plans envision economic growth of six percent a year through 2020 and continuing rapid growth thereafter. But these ambitious visions seem to ignore the fact that the country has been in the grip of a protracted demographic crisis since the end of communist rule. Since 1992, Russia's deaths have outnumbered births by roughly 50 percent, or about 13 million, and official figures suggest that the country's population has shrunk by about five percent – nearly seven million people – from 148.6 million in 1993 to 141.9 million today. Immigration has helped slow the country's population decline but has not been able to prevent it. The outlook is for further depopulation: medium variant projections by the Kremlin's official statistical service envision ten million more deaths than births over the next two decades.

Even more troubling for Russia is the country's disastrous public health situation. In 2009, as hard as it may be to believe, Russia's overall life expectancy was a bit lower than it had been in 1961, almost half a century earlier. To make matters worse, at least from an economic standpoint, Russia's health crisis is concentrated in its working-age population. Over the 40 years between 1965 and 2005, for example, the death rates for men between their late 20s and their mid-50s virtually doubled. Death rates for women in that same age group generally rose by about 50 percent. Public health experts do not entirely understand the reasons for this death spiral – although poor diet, smoking, sedentary lifestyles, and, above all, Russia's deadly romance with vodka can explain much of the deterioration, the actual decline is worse than what these risk factors alone would suggest. In some respects, contemporary health levels for Russian adults are akin to those for adults in the world's most impoverished states. According to estimates by the World Health Organization, life expectancy for a 15-year-old man in 2008 would have been lower in Russia than in Cambodia, Eritrea, or Haiti. Between now and 2030, the U.S. Census Bureau projects that Russia's working-age population will fall by nearly 20 percent, and Russia's work force will almost surely suffer more ill health than its counterparts in the OECD and than the work forces of the other BRIC countries (Brazil, India, and China). In 2008, according to World Health Organization estimates, mortality levels for Russia's working-age population were 25 percent higher than those for India's.

Urban centers are typically the hubs of economic growth, but Russia's urban population is smaller today than it was at the end of the communist era, and the UN projects that there will be even fewer inhabitants in Russia's cities 20 years from now. In addition, Russia's old-age burden will be steadily increasing – whereas 13 percent of the Russian population today is 65 or older, the projected proportion for 2030 is 21 percent. Taking all the above into account, it is difficult to see how Russia can hope to generate sustained and rapid economic growth on the basis of its human resources. Natural resources may offer the country economic opportunities in the years ahead, but these opportunities should not be exaggerated. Despite all of Russia's energy and mineral wealth, its annual export earnings have never exceeded those of Belgium, not even at the height of the pre-crisis oil boom.

India's GDP growth has averaged an impressive 6.5 percent a year since the economic reforms that began in 1991. Recently, the economy has been humming along at eight percent growth per year. Not a few observers think the best may be yet to come. In just one example, a member of India's Planning Commission suggested in 2008 that India's economy would be growing at eight to nine percent a year for the next quarter century. In the same time frame, India's total population is set to grow by just over one percent per year, and about five-sixths of that growth will be in its working-age population. Thanks to the disproportionate growth of India's manpower pool, the country's dependency ratio (the ratio of children under 15 and persons over 65 to the working-age population) will be falling, and the society will remain relatively youthful. Such changes in population structure could facilitate higher levels of national savings and investment – and, thus, economic growth. In short, India appears to be a poster child for a potential demographic dividend.

But India has striking regional disparities in population profiles. India is bisected by a great north-south fertility divide: in much of the north, including parts of the Ganges river belt and some of the country's westernmost districts, fertility levels remain quite high, at four, five, or more children per woman; in much of the Indian south, however, fertility levels are at, or already below, the replacement level. In effect, this means that two very different Indias are being born today -- a youthful, rapidly growing northern India whose future population structure will be akin to that of a traditional Third World society and a southern India whose population growth will be slowing or ceasing, where manpower growth will be coming to an end, and where pronounced population aging will be taking hold.

This demographic divergence could make sustaining rapid economic growth a trickier proposition than it might seem at first. India's engines of economic growth are mainly its sub-replacement-fertility areas, which include much of the south and practically all its major urban centers: Bangalore, Chennai, Kolkata, and Mumbai. But its demographics mean that the country's future workers will increasingly come from the high-fertility areas of the north. This reveals a fundamental mismatch: India's continued economic growth requires workers who are relatively well educated, but India's mostly rural high-fertility areas are producing a rising generation with woefully low levels of schooling.

India, it is true, can boast of a cadre of millions of highly trained engineers, scientists, researchers, and professionals. But in a country of well over a billion people, these specialists compose only a tiny fraction of its overall manpower. In the country as a whole, educational levels are still remarkably limited, and remedial efforts will take generations to achieve substantial improvement. Currently, about a third of India's working-age population has no education at all; 20 years from now, a sixth of the country's work force may still be totally unschooled. These educational shortfalls place material constraints on the prospects for sustaining rapid rates of economic growth.

Broadly speaking, all the developed economies will face demographic slowdowns and population aging in the coming decades, but Japan stands to be the most heavily burdened by the looming trends. It has had the steepest and longest fertility falloff in modern history. In 2008, the country recorded around 40 percent as many births as it had 60 years earlier. Japanese childbearing is currently estimated to be nearly 35 percent below the replacement level. But Japan has also enjoyed rapid and continuing improvements in public health since the end of World War II. The Japanese have an average life expectancy of 83 years, higher than any other country in the world. Taken together, the country's fertility, migration, and mortality trends are propelling Japan into demographic decline, and into a degree of aging thus far contemplated only in science fiction.

Over the next two decades, according to U.S. Census Bureau estimates, the surfeit of deaths as compared to births is expected to drive Japan's total population down from 127 million to 114 million, a ten percent decrease. The relative decline in the working-age population is projected to be even steeper, from 81 million to 67 million, or a 17 percent decrease. All the while, the number of Japanese senior citizens would be rising -- and by 2030, the country's median age will be above 52 years, with 30 percent of the total population 65 or older. The economic implications of these impending changes are far from positive. Even with healthy aging and later retirement, these trends suggest a marked contraction in the country's labor supply. Moreover, the social and economic strains from Japan's looming old-age boom could further complicate efforts to maintain even the country's current sluggish rates of economic growth.

Western Europe, for its part, can expect population stagnation, according to the U.S. Census Bureau -- its population may grow by just three percent over the next two decades, with near-zero growth projected by 2030. Germany and Italy are expected to experience population decline. A stagnating Europe will also be a graying Europe. The U.S. Census Bureau estimates that western Europe's median age would rise from 42 years today to nearly 46 years by 2030. Despite overall population stagnation, western Europe's 65-and-older population is set to rise by nearly 40 percent, while its manpower pool is slated to shrink by 12 million people. And these projections are premised on a net inflow of approximately 20 million immigrants, mainly of working age.

Two unanswered demographic questions loom over the future of the western European economy. First, can the countries in the region succeed in attracting and incorporating the foreign workers their economies will need in the coming decades? Thus far, western Europe's record on the social inclusion of immigrants may have been somewhat better than many appreciate; however, there have been increasing assimilation problems, which, if left unattended, could impinge on economic growth, as well as social cohesion. Second, can the countries of western Europe translate public health improvements into longer working lives for progressively aging populations? At the moment, overall life expectancy at birth in western Europe is about two years higher than in the United States (80 years compared to 78 years). But the average retirement age in western Europe is lower than it is in the United States, even despite recent increases in the labor-force participation of older workers in northern Europe. This summer's public protests in France against a proposed increase in the French retirement age from 60 to 62 shows how tough it may be to achieve political consensus.

THE DEMOGRAPHIC EXCEPTION

The United States will avoid the demographic stagnation and decline that faces most other OECD countries. The U.S. population, according to U.S. Census Bureau projections, is set to grow by 20 percent, or over 60 million people (from 310 million to 374 million), between 2010 and 2030. By such projections, the United States' population growth rate will nearly match India's. According to these calculations, the United States' rate of population growth approximates that of the world's average, meaning that the U.S. share of global population is not set to shrink. Virtually every age group in the United States is set to increase in size over the next 20 years. Unlike all other affluent countries, the United States can expect a growing pool of working-age people (a moderate but steady rise averaging 0.5 percent per year over the next 20 years), and it can expect a slower pace of population aging than virtually any other state in the OECD.

The United States' demographic exceptionalism is explained by the country's relatively high fertility rate and its continuing influx of immigrants. Over the past generation and a half, while fertility rates in most other Western countries were plunging, the fertility rate in the United States was actually increasing, and unlike that of any other large rich country, its rate has been hovering just around the replacement level for the past generation. If fertility and immigration in the United States remain more or less at their current rates, as U.S. Census Bureau projections assume they will, the United States will enjoy a surplus of births over deaths of nearly 35 million and will tally a net inflow of almost 30 million immigrants over the next 20 years. Both factors would keep the nation growing and relatively young, shaping a distinctly more auspicious outlook for economic growth in the United States than exists for Japan or western Europe.

Nevertheless, there are also clouds on the U.S. demographic horizon, all of them regarding the quality of future U.S. human resources. The

United States has a relatively good record when it comes to assimilating immigrants as productive newcomers, but resistance to continued immigration, or unexpected new problems in absorbing immigrant inflows, could limit future success. Furthermore, the United States' primary and secondary public education system produces uneven results that are mediocre in comparison to other affluent societies. The percentage of Americans graduating from high school has been slowing and could possibly plateau in the years ahead. And advances in health in the United States do not compare well with those under way in other affluent states. Education and health will be key to enhancing the productivity and wealth of the U.S. population in the decades ahead, which means there are few grounds for complacency when contemplating these challenges.

Despite the particular differences in their demographic outlooks, Japan, western Europe, and the United States share a common fiscal problem: the relationship between population aging and public-debt obligations. Over the past two decades, a striking feature has emerged in the macroeconomies of the OECD countries. The gross burden of public debt as a proportion of GDP has come to correspond with the proportion of the population that is 65 or older. Very roughly speaking (as my colleague Hans Groth and I have shown), costs associated with population aging are estimated to account for about half the public-debt run-up of the OECD economies over the past 20 years. In the next two decades, the increase in the 65-and-older population will be about twice as great as it was in the decades just past. Coping with the fiscal and public-debt implications of the pressures that population aging places on macroeconomic performance may not be an entirely new challenge for affluent societies, but it promises to become an ever more salient one over the next 20 years.

HUMANITY'S SECRET WEAPONS

Left unattended, the global demographic trends outlined above suggest serious and gradually mounting pressures on global economic development and may lead to downward revisions of worldwide material expectations. But feasible options do exist to alleviate some of these pressures -- and to capitalize on new demographic opportunities that may arise. Addressing these new demographic challenges will require deliberate, concerted, and sustained efforts. Such an approach must focus on augmenting human capital by expanding education, improving health conditions, and creating an economic environment in which greater returns can be generated by the world's precious human resources.

Improving educational opportunity and quality in low-income areas, for example, should figure centrally in enhancing prospects for local and global growth. Better-educated workers tend to be not only more productive but also healthier and better placed to lead longer working lives. Simply put, populations in developing countries cannot hope to generate First World income levels with Third World educational profiles. Improving health status should also be a central objective, since health advances could prove critical to maintaining or increasing long-term economic growth rates in an ever-graying world.

For affluent, graying societies, taking economic advantage of healthy aging will become ever more crucial to the quest for higher national income levels. This suggests that the existing disincentives in so many rich countries to continuing to work at older ages should be reexamined and ultimately eliminated. At the same time, governments should consider careful incentives for the voluntary extension of working life. More generally, in both rich and poor countries, governments should enact business and economic policies that enhance the efficiency of manpower resources, thereby eliciting higher productivity and faster economic growth.

Humanity has one additional "secret weapon" in accelerating growth in the years ahead: knowledge production and technological innovation. The revolutions of the past generation in health and life sciences, information technology, and materials science point to the sorts of opportunities that may lie ahead for improving productivity. More than ever before, research and development must be incentivized to reward risk takers.

For the sake of the world's future prosperity, reforms and innovations must be pursued with urgency. Demographic changes unfold slowly from month to month, but the cumulative impact can be staggering. It is not alarmist to warn that there is no time to lose in recognizing -- and adapting to -- the enormity of the world's unavoidable demographic challenges.

NICHOLAS EBERSTADT is Henry Wendt Chair in Political Economy at the American Enterprise Institute and Senior Adviser to the National Bureau of Asian Research.

Copyright © 2002-2010 by the Council on Foreign Relations, Inc. All rights reserved.

[Back To Table Of Contents](#)

36. Can the CIA still accomplish its mission?

Charles Faddis, CNN.com, 26 October 2010

Special to CNN

(CNN) -- On October 19, the Central Intelligence Agency made public the results of the inquiry by its counterintelligence division into the December 30 bombing of its Khost base in Pakistan and the killing of seven Agency officers.

There were two key findings. First, it was established that significant errors in tradecraft were made and that these led to the deaths of the officers in question. That much had been clear for 10 months.

The second determination was more controversial. It was that all of the errors were the result of reasonable decisions by individuals involved in the conduct of the operation.

Accordingly, it was announced that there would be no disciplinary action and that no one connected to the operation would be relieved or reassigned. Rather, lessons learned would be assessed, new procedures implemented and new bureaucratic entities created within the CIA to provide additional insight and layers of review in regard to high-profile and high-risk operations.

As President Obama is fond of saying, let me be clear. Nothing that happened at Khost Base and resulted in the deaths of the officers in question was the product of a reasonable decision.

What happened at the Khost Base was the product of a succession of inexcusable errors:

A chief of base, who was a highly skilled and very talented headquarters staff officer but who lacked any real operational field experience, was sent to command one of the CIA's most dangerous posts.

Excessive reliance was placed on the estimations and opinions of a foreign liaison service with which the CIA was cooperating. Multiple layers of command stretching from Kabul to Washington interfered in the running of the case and muddled the waters as to who was in charge of what aspects of the case.

Key tactical decisions such as whether to search a source in a war zone were debated in Amman and Washington rather than being left to the judgment of the commander on the scene.

A clandestine source of uncertain loyalty, in direct contact with members of al Qaeda, was picked up and brought into a secure facility and placed in immediate proximity to virtually the entire complement of a secret CIA base without being searched or subjected to any other measures to screen for weapons or explosives. The source, a Jordanian, detonated explosives, killing himself and seven CIA officers.

The greenest graduate of the Farm, the CIA's training facility, could look at those factors and tell you that they are a prescription for disaster and a good way to get people killed. There is not a case officer worth his or her salt within the CIA today who does not know that what happened at Khost was inexcusable. Anyone who argues to the contrary is either ignorant of the tradecraft used in the conduct of high-risk meetings or deliberately misrepresenting the facts.

Unfortunately, Khost is not an aberration. It is a symptom of what is wrong with the CIA today. It is an organization staffed by thousands of dedicated, patriotic Americans, but it is a broken, dysfunctional entity against which those same Americans must struggle everyday to do their jobs.

Senior leadership is generally poor and focused more on self-preservation and advancement than mission accomplishment. Few, if any, of the senior officers involved in planning the Khost operation have ever conducted the kind of high risk meeting that lead to that debacle. The bureaucracy is stiff, risk-averse and increasingly filled with individuals who see the CIA as simply another federal job rather than the unique and special place it once was.

The Clandestine Service, the core of the CIA, has been de-professionalized and stripped of the elite status it once enjoyed. It is now staffed in large measure not by seasoned overseas operators but by new hires, former support personnel and headquarters-based desk officers.

The solution to all this is not more bureaucracy and more studies. It is not the imposition of requirements for yet more deliberation and review. It is the restoration of standards and accountability. We are in the middle of a war. We cannot afford half measures and dithering. The CIA as it currently exists is not capable of grappling with the kinds of enemies against which we are now engaged. We need to fix that and quickly.

Whether change on the scale it needs to happen can occur within the confines of today's CIA or necessitates the creation of a new organization entirely is a matter for debate. I personally believe that repair is impossible and that replacement is required. Regardless, tinkering and minor adjustment will not get the job done. Reform on a massive scale is necessary.

This president came to office promising change and a fresh, pragmatic look at the problems our nation faces. Nine years after September 11, with Osama bin Laden still at large and in the wake of the Khost Base debacle, it is time to bring that kind of change to the CIA. The fallen deserve no less.

Editor's note: Charles S. Faddis is a retired CIA operations officer and the former head of CIA's WMD terrorism unit. He is the author of several works of nonfiction, including "Beyond Repair," an argument for the creation of a new intelligence agency modeled on the World War II-era OSS.

The opinions expressed by this commentary are solely those of Charles S. Faddis.

© 2010 Cable News Network

[Back To Table Of Contents](#)

UNCLASSIFIED

37. SpyTalk: NYU gets the papers of Philip Agee, renegade CIA agent

Jeff Stein, Washington Post, 27 October 2010, Page A21

NYU library acquires the papers of Philip Agee, renegade spy

The private papers of Philip Agee, the disaffected CIA operative whose unauthorized publication of agency secrets 35 years ago was arguably more damaging than anything WikiLeaks has produced, have been obtained by New York University, which plans to make them public next spring.

Agee, who worked undercover in Latin America from 1960 to 1968 and died in Cuba nearly three years ago, once said he resigned because the values of his Catholic upbringing clashed with his CIA assignments to destroy movements that aimed to overthrow U.S.-backed military regimes. CIA defenders said he was on the verge of being fired.

Agee's first book, "Inside the Company: CIA Diary," published in 1975, included a 22-page appendix with the real names of about 250 undercover agency operatives and accused a handful of Latin American heads of state of being CIA assets. The CIA's classified in-house journal, Studies in Intelligence, called it "a severe body blow" to the agency.

Two subsequent books by Agee and Louis Wolf revealed the names of about 2,000 more alleged CIA operatives in Western Europe and Africa.

After the release of "Inside the Company," Congress passed legislation making it a crime to intentionally publish the names of undercover CIA personnel.

In contrast to Agee, WikiLeaks withheld the names of hundreds of informants from the nearly 400,000 Iraq war documents it released over the weekend, according to news reports. And its previous surfacing of Afghan war documents, which an Army specialist is suspected of leaking, did not reveal "any sensitive intelligence sources and methods," according to Defense Secretary Robert M. Gates.

Agee may have started out as an independent whistleblower, but according to retired KGB Maj. Gen. Oleg Kalugin, the ex-operative offered CIA documents to the Soviet Embassy in Mexico City in 1973. Suspecting a ruse, the KGB turned him down, Kalugin said. Agee denied that he worked for the Russians, but he openly enlisted Cuba's help in his campaign to neutralize CIA operations against leftists and trade unions in Latin America.

NYU's Tamiment Library, which acquired Agee's papers from his widow, Giselle Roberge Agee, made no mention of the renegade agent's KGB and Cuban intelligence connections in its Monday news release.

But it did maintain that "for the rest of his life Agee was a target of CIA assassination threats."

In response to a query, Michael Nash, the library's associate curator, said, "This information came from the Agee book 'On the Run,' and it is supported by some CIA documents that Agee received as a result of a Freedom of Information Act request."

A CIA spokesperson, speaking on the condition of anonymity, dismissed the allegation as "not only wrong, but ludicrous."

NYU said the acquisition of the Agee collection will be celebrated with a Nov. 9 reception, but the papers will not be available until April.

They include "legal records, correspondence with left-wing activists, mainly in Latin America, and others opposed to CIA practices and covert operations; papers relating to his life as an exile living and working in Cuba, Western and Eastern Europe; lecture notes, photographs, and posters," the library said.

"Mrs. Agee donated the collection to Tamiment because we have an international reputation as a repository documenting the history of left politics and the movement for progressive social change," Nash said in the library's statement.

© 2010 The Washington Post Company

[Back To Table Of Contents](#)

UNCLASSIFIED

38. U.S. Lost Communications With 50 Nukes

Julian E. Barnes, Wall Street Journal, 27 October 2010, Page A3

Communications with some 50 nuclear missiles were disrupted for 45 minutes on Saturday, making it more difficult to launch them and sending the military scrambling to determine the cause of the incident, according to defense officials.

The incident was significant enough that President Barack Obama was briefed on it this week.

A defense official said a power failure disrupted communications between a control center and the missiles at F.E. Warren Air Force Base in Wyoming.

There was no danger of an accidental launch, officials said, and the Air Force had eyes on the missiles at all times. "There was no threat to the public," said the defense official. The cause of the power failure remains unknown, but it is not believed to be malicious.

Adm. Michael Mullen, the chairman of the joint chiefs of staff, notified Defense Secretary **Robert Gates** of the incident. The incident was first reported by the Atlantic on its website on Tuesday.

Another official said the cause of the incident was being analyzed. "The missiles were protected by multiple, redundant safety security and control features," said a military official.

In 2008, a series of problems with nuclear weapons and parts, including the accidental transport of a weapon across the U.S., led Defense Secretary Gates to fire the Air Force secretary and chief of staff.

The current Air Force leadership has put more emphasis on improving nuclear readiness and stewardship of the arsenal. It has restored funding, increased the number of inspections, and tried to increase the prestige of airmen and officers working in the nuclear field.

The Atlantic reported that the squadron of ICBMs was in "LF Down" status, which means the airmen in the missile bunkers could not communicate with the missiles.

The missiles still could be launched, but only by airborne command and control platforms. Although the missiles at Warren Air Force base represent a large proportion of the ICBM arsenal, the defense official said that at no time was Mr. Obama without a nuclear-launch capability.

Copyright 2009 Dow Jones & Company, Inc. All Rights Reserved

[Back To Table Of Contents](#)

UNCLASSIFIED

39. **FBI** links shots fired at Pentagon, Marine museum

Josh White and Maria Glod, Washington Post, 27 October 2010, Page A1

Two shootings that targeted U.S. military buildings in Northern Virginia have been conclusively linked to the same weapon, and law enforcement officials think a third attack on a Marine Corps recruiting office this week could be part of the same unexplained spree.

Law enforcement officials announced Tuesday that ballistics tests linked bullets found at the National Museum of the Marine Corps in Triangle on Oct. 17 with evidence found at the Pentagon two days later. Both buildings are within range of busy interstate highways and are about 30 miles apart.

Law enforcement officials declined to discuss the type of weapon used in the shootings or the caliber of ammunition, but they have said previously that they believe the rounds were fired using a high-velocity rifle.

The **FBI**'s Joint Terrorism Task Force has taken the lead in the investigation. Agents are working to do ballistics testing on material found at the scene of a shooting at a Marine Corps recruiting office in a Chantilly shopping center late Monday or early Tuesday. A Marine Corps recruiter found two bullet holes in the office's windows at 8:30 a.m. Tuesday, although a Marine Corps official said the office has been closed for renovations.

Police say they are unsure what is motivating the shootings, and they are reluctant to speculate.

"We are working with local law enforcement to determine anything we can to provide us any clues," said Lindsay Godwin, a spokeswoman for the **FBI**'s Washington field office. "I don't think at this point in time we are prepared to say this is a serial of any kind. But the targets are all blatantly military."

Although the Terrorism Task Force is leading the investigation, officials described that as a precaution because of the military targets. It is unclear whether the shootings are acts of terrorism.

The unknown shooter - or shooters - have targeted buildings late at night or early in the morning, when the buildings were either unoccupied or there was little chance of people being around. Police said that the attacks essentially amount to vandalism but that they are troubling and mysterious.

"So far, no one has been injured, so we don't have a reason to believe that they're trying to hurt someone, whoever this is," said Chris Layman, a spokesman for the Pentagon Force Protection Agency. "But it is a cause for concern that someone would be doing this."

Steven Weber, a political science professor at the University of California who has studied terrorist behavior, said investigators must consider a wide range of possibilities.

"It could be someone who holds a grudge against the military. It could be someone who believes by targeting military facilities they will get a lot of attention. It could be someone suffering from PTSD [post-traumatic stress disorder] who believes someone in one of those buildings is responsible," Weber said. "Or it could be none of those things."

Spokesmen for the Marine Corps and the defense secretary's office declined to comment on the shootings Tuesday, referring calls to law enforcement officials.

The first shooting targeted the National Museum of the Marine Corps on Oct. 17. A cleaning crew discovered bullet holes in upper-level windows at the museum, whose design was inspired by the Iwo Jima Memorial and which can be seen rising above the trees along Interstate 95 near Quantico Marine Base.

Prince William County police searched Interstate 95 looking for clues last week and think that the shots probably were fired from the direction of the highway. Prince William Deputy Police Chief Barry Barnard said Tuesday that it was too early to speculate about a motive for the shots.

"At this stage, we don't know what anyone's intentions are, but we're certainly taking it seriously," Barnard said.

Two days after the shooting in Triangle, audible shots were reported at the Pentagon about 4:30 a.m., emanating from the direction of the south parking lot, which lines Interstate 395.

Two windows at the Pentagon were hit, and authorities analyzed bullet fragments taken from those windows. The damaged windows led to rooms that were unoccupied and are under renovation.

Fairfax County police said Tuesday that they were called to 13881 MetroTech Drive at 8:30 a.m. to investigate a vandalism at the Marine Corps recruiting office. Lucy Caldwell, a police spokeswoman, said an employee discovered two bullet holes in a window and one in an adjacent business.

"The target in the shooting appears to have been unoccupied buildings," Caldwell said.

Marine Sgt. Athanasios Genos, marketing and public affairs chief for the Frederick recruiting station, said the Chantilly location is a substation that has been closed for renovations and was unoccupied. Genos said a recruiter stopped by the office Tuesday and found the bullet holes.

"The office is down for renovations, and no one is working there right now," Genos said. "It is a recruiting station, but it's not currently being used due to internal renovations. I don't know if someone would know that from the outside."

Staff writer Jerry Markon and staff researcher Julie Tate contributed to this report.

© 2010 The Washington Post Company

UNCLASSIFIED