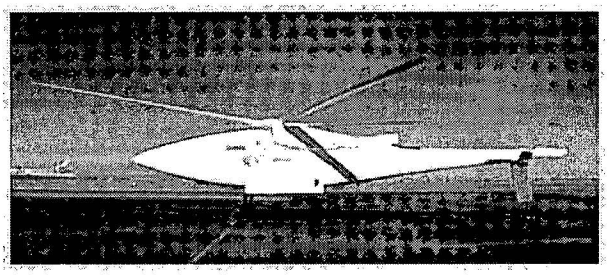
DARPA MISSION

DARPA's mission is to maintain the technological superiority of the U.S. military and prevent technological surprise from harming our national security by sponsoring revolutionary, high-payoff research bridging the gap between fundamental discoveries and their military use.

Over the years, DARPA has worked to enhance our national security by funding research and technology development that not only have improved our military capabilities but have changed the way we live. Since the very beginning, DARPA has been the place for people with innovative ideas that lead to groundbreaking discoveries.

Learn more about DARPA's history of innovation.



b6
b7C

[redacted]

From: [redacted]@darpa.mil]
Sent: Tuesday, January 26, 2010 1:56 PM
Cc: [redacted]
Subject: DARPA Public Release: A New Fundamental Search Tool

University-based research is an important component of DARPA's activities. It is our goal to strengthen the partnership in the best interests of the Nation and the U.S. Department of Defense.

DARPA is challenging itself to provide accurate and timely information on the release or requirement for pre-publication review, ITAR and foreign national restrictions, as well as other perceived or actual constraints on fundamental research.

We have this week launched a Search tool that allows performers to determine whether or not their Prime Award requires them to submit materials for pre-publication review.

This Search tool can be found at DARPA's new Public Release Center (formerly known as TIO) at:
http://dtsn.darpa.mil/fundamentalresearch/

Our performers and researchers share the responsibility in this effort by ensuring publications are consistent with the defined research scope (not discussing potential uses for example) and continuously monitoring fundamental research for statement of work creep or unanticipated breakthroughs.

In the case that material does require pre-publication review, we ask for at least 20 days notice (or what is detailed in your contract).

Please contact me with any questions or comments about this effort. Thank you.

[redacted]

[redacted]
DARPA External Relations
[redacted](phone)
(fax)
darpa.mil
www.twitter.com/DARPA_news

Skip to Content
Fundamental Research

Home

Public Release Process

Submit a Request

Press Releases

Distribution Statements

DoD Directives, Policies and Procedures

Contact Information

Frequently Asked Questions

Does your award have a pre-publication review requirement?

DARPA's Prime Award Number:
(e.g. HR001109C1234)

Your Information:

Name:

Email:

Organization:

Search

This database is a resource for those performing fundamental research with DARPA and contains awards beginning in 2007.
Detailed guidance about pre-publication review can be found in your contract/award.

DARPA's Fundamental Research Overview

For questions or comments, please contact External Relations.

ROOM 415 3701 N.FAIRFAX DRIVE ARLINGTON, VA 22203 571-218-4235 PRC@DARPA.MIL

China Removed As Top Priority For Spies

The Washington Times

By Bill Gertz

January 20, 2010

WASHINGTON, DC -- The White House National Security Council recently directed U.S. spy agencies to lower the priority placed on intelligence collection for China, amid opposition to the policy change from senior intelligence leaders who feared it would hamper efforts to obtain secrets about Beijing's military and its cyber-attacks.

The downgrading of intelligence gathering on China was challenged by Director of National Intelligence Dennis C. Blair and CIA Director Leon E. Panetta after it was first proposed in interagency memorandums in October, current and former intelligence officials said. The decision downgrades China from "Priority 1" status, alongside Iran and North Korea, to "Priority 2," which covers specific events such as the humanitarian crisis after the Haitian earthquake or tensions between India and Pakistan. The National Security Council staff, in response, pressed ahead with the change and sought to assure Mr. Blair and other intelligence chiefs that the change would not affect the allocation of resources for spying on China or the urgency of focusing on Chinese spying targets, the officials told The Washington Times.

White House National Security Council officials declined to comment on the intelligence issue. Mike Birmingham, a spokesman for Mr. Blair, declined to comment. A CIA spokesman also declined to comment. But administration officials, speaking on the condition of anonymity, said the new policy is part of the Obama administration's larger effort to develop a more cooperative relationship with Beijing. A U.S. official who defended the policy change said "everybody involved understood the absolute importance of China as an intelligence priority." "This is a case in which the assignment of a relative number — one or two — wouldn't mean, or change, a damn thing. And it didn't." The official said the U.S. government "has to keep its eyes on a host of threats, challenges and opportunities overseas. That's how it works."

Critics within the government, however, said the change will mean that strategic intelligence on China — the gathering of data and analysis of information — will be reduced over time, undermining what officials said are urgently needed efforts to know more about China's political, economic, military and intelligence activities. Rep. Peter Hoekstra of Michigan, the ranking Republican on the House Permanent Select Committee on Intelligence, expressed concern about the change. "For those who say changing from Priority 1 to Priority 2 doesn't make any difference — well then, why do it?" he asked. "China should be at the top of the priority list, not moving down." Officials said the lower intelligence priority for China is a subtle but significant change that will affect an array of intelligence activities.

Although the effect is not expected to be immediate, a change in priority number generally means that projects regarding that country are scrutinized more skeptically on budgetary and other grounds. Agencies likely will reduce spending for intelligence operations on China, whether carried out by spies or by photographic and electronic-intercept satellites. Critics of the decision also fear that the lower priority will cause CIA and Defense Intelligence Agency operatives to take fewer risks in the field when spying on Chinese targets. One new area that has been given a higher intelligence priority under the Obama administration is intelligence

collection on climate change, a nontraditional mission marginally linked to national security. The CIA recently announced that it had set up a center to study the impact of climate change.

One U.S. official said the NSC intelligence policy change followed protests from China's government about the publication in September of the National Intelligence Strategy, produced by Mr. Blair's DNI office. The strategy report identified China as one of four main threats to U.S. interests, along with Russia, Iran and North Korea. At the time of its release, Mr. Blair was asked by reporters about the strategy report's harsh assessment of China and efforts to increase intelligence gathering on China. "I would say that it is a muscular intelligence response to meet the nations responsibilities so that we can provide good advice to the policymakers and in the field," he said.

The Chinese government reacted harshly to the strategy report, both in public and in diplomatic channels, the official said. A Chinese government spokesman in September stated that "we urge the United States to discard its Cold War mindset and prejudice, correct the mistakes in the [National Intelligence Strategy] report and stop publishing wrong opinions about China which may mislead the American people and undermine the mutual trust between China and the United States." The NSC downgrading of China from so-called "Pri-1" to "Pri-2" was a political decision by the Obama administration that was designed to assuage Chinese concerns that intelligence agencies were exaggerating the threat from Beijing, the official said.

John Tkacik, a former State Department intelligence official, said the demotion of China to a second-tier priority reflects bias within the NSC staff. "It means that the Obama administration doesn't understand the profound challenge that China has become or, even more disturbing, it cannot understand that China's challenges to America's policies are becoming even more threatening with each passing week," he said. The intelligence downgrade was disclosed as civilian and military leaders were calling U.S. intelligence collection and analysis on China deficient.

Adm. Robert Willard, the new commander of U.S. Pacific Command, indirectly criticized U.S. intelligence estimates on China last fall, telling reporters in November that during the past decade "China has exceeded most of our intelligence estimates of their military capability and capacity every year. They've grown at an unprecedented rate in those capabilities." Mr. Hoekstra said he had not been briefed in advance about the NSC's new policy on China intelligence gathering. But the shift sends the wrong signal to the 16 agencies that make up the U.S. intelligence community that China is not important, he said in an interview.

"That's a wrong analysis," Mr. Hoekstra said. "The current situation with China is that they are cheating on trade agreements, aggressively pursuing military capabilities and aggressively conducting cyber-attacks." A military official also said recently that Army, Air Force and Navy intelligence components are just beginning to understand the growing need to focus more intelligence assets on the challenges posed by China's military buildup and aggressive intelligence activities. Counterintelligence officials also were surprised at the decision to lower the intelligence priority on China, noting that China's espionage, technology theft and economic spying continue to dominate scarce resources, including people and funds.

Michelle Van Cleave, former national counterintelligence executive, also said the priority change was ill-advised and will hurt personnel, funding and intelligence assets devoted to Chinese targets. "Chinese intelligence is going after us with a vengeance," she said, noting that the problem includes industrial espionage, technology diversion and stealing defense and other

national security secrets, in addition to a global campaign of cyber-espionage. "So why are they doing this?" she asked. "I am very troubled by how little U.S. intelligence really knows about the Chinese, in part because they have been so successful against us. Our national leadership should be pushing to close this intelligence gap, because if they don't, they will risk making serious miscalculations in dealing with China."

The Washington Post

Google China cyberattack part of vast espionage campaign, experts say

By Ariana Eunjung Cha and Ellen Nakashima
Thursday, January 14, 2010; A01

Computer attacks on Google that the search giant said originated in China were part of a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of major financial, defense and technology companies and research institutions in the United States, security experts said.

At least 34 companies -- including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical -- were attacked, according to congressional and industry sources. Google, which disclosed on Tuesday that hackers had penetrated the Gmail accounts of Chinese human rights advocates in the United States, Europe and China, threatened to shutter its operations in the country as a result.

Human rights groups as well as Washington-based think tanks that have helped shape the debate in Congress about China were also hit.

Security experts say the attacks showed a new level of sophistication, exploiting multiple flaws in different software programs and underscoring what senior administration officials have said over the past year is an increasingly serious cyber threat to the nation's critical industries.

"Usually it's a group using one type of malicious code per target," said Eli Jellenc, head of international cyber-intelligence for VeriSign's iDefense Labs, a Silicon Valley company helping some firms investigate the attacks. "In this case, they're using multiple types against multiple targets -- but all in the same attack campaign. That's a marked leap in coordination."

While it's difficult to say with certainty where a cyberattack originated because the Internet allows hackers to seemingly crisscross country borders and time zones in seconds, the issue is quickly turning into a source of diplomatic tension.

The standoff between Google and China touches on the most sensitive subjects in U.S.-China relations: human rights and censorship, trade, intellectual property disputes, and access to high-tech military technology.

"The recent cyber-intrusion that Google attributes to China is troubling, and the federal government is looking into it," White House spokesman Nick Shapiro said. He added that President Obama made Internet freedom "a central human rights issue" on his trip to China last fall.

Since it began operations in China five years ago, Google had agreed in theory to filter sensitive searches but clashed with the Chinese government on what material was covered, and the company regularly found its service blocked when it defied its hosts.

China's state media reported that the government is looking into Google's claims. In China, news about Tuesday's public rebuke by Google was heavily censored except for a stinging opinion piece in the official People's Daily that called the Silicon Valley tech giant a "spoiled child" and predicted that it would not follow through on its ultimatum.

The recent attacks seem to have targeted companies in strategic industries in which China is lagging, industry experts said. The attacks on defense companies were aimed at gaining information on weapons systems, experts said, while those on tech firms sought valuable source code that powers software applications -- the firms' bread and butter.

The attacks also focused on obtaining information about political dissidents.

"This is a big espionage program aimed at getting high-tech information and politically sensitive information -- the high-tech information to jump-start China's economy and the political information to ensure the survival of the regime," said James A. Lewis, a cyber and national security expert at the Center for Strategic and International Studies. "This is what China's leadership is after. This reflects China's national priorities."

Adobe, a software maker, confirmed on Wednesday that it learned of the attacks on Jan. 2 but said there was "no evidence to indicate that any sensitive information . . . has been compromised," while Symantec, which makes security software, said it is investigating to "ensure we are providing appropriate protection to our customers."

Dow Chemical said that it has "no reason to believe that the safety, security and intellectual property of our operations are in jeopardy." Yahoo and defense contractor Northrop Grumman declined to comment on the attack.

The attackers, experts said, followed the familiar "phishing" ruse: A recipient opens an e-mail that purports to be from someone he knows and, not suspecting malicious intent, opens an attachment containing a "sleeper" program that embeds in his computer. That program can be controlled remotely, allowing the attacker to access e-mail, send confidential documents to a specific address -- even turn on a Web camera or microphone to record what is going on in the room.

In many cases, a user does not know he has been the victim of an attack.

One type of attack exploits a flaw in Adobe Reader, a popular free program that allows e-mail users to read .pdf document files. The flaw was made public Dec. 15 but fixed only on Tuesday -- the day Google announced that its systems had been compromised.

Sara L.M. Davis, executive director of New York-based Asia Catalyst, which assists charities in developing countries, said she began to receive these fake e-mails shortly after the new year. The

senders all appeared to be people with whom she regularly communicates. The subject lines contained topics -- "AIDS in China" or "Some photographs of you and Dr. Gao" -- that suggested familiarity with her and her organization.

"If I weren't already paranoid, I would have already opened one," Davis said.

Google declined to provide details on what exactly the attackers took and whether it included any information about super-secret search engine technology that drives the company's profits.

Nart Villeneuve, a research fellow at the University of Toronto, has analyzed attack e-mails sent to human rights groups over the past few months. Villeneuve, who works at Citizen Lab, which focuses on Internet and politics, helped research GhostNet, a vast cyberspying operation revealed last year that apparently originated in China and targeted the office of the Dalai Lama, foreign embassies and government offices.

He said the GhostNet attack resembles the strategy used against Google, other U.S. companies and human rights groups this time around. The attack e-mails to the human rights organizations could mostly be traced to "command and control" computers in mainland China. However, Jellenc said, the two attacks do not appear to have been carried out by the same group.

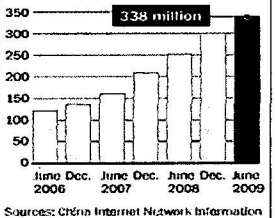
In August, someone obtained a list of 5,000 subscribers to the China Leadership Monitor, a respected quarterly publication from the Stanford University's Hoover Institution.

The subscribers received a fake e-mail from a Gmail account purportedly from the publication but with an attachment that would take over their computers. Alice Miller, a visiting professor at Stanford and the publication's editor, said she had worked with U.S. government investigators and said the attack originated in China.

Staff writers Cecilia Kang and John Pomfret contributed to this report.

What Google might miss out on

Google said it may exit China, the world's largest Internet market, after a series of cyberattacks. Google continued to gain search-engine market share in China in 2009 from leader Baidu. Google derives an estimated $300 million to $400 million in annual revenue from China's Internet users.



Sources: China Internet Network Information Center, Bloomberg
The Washington Post