

HENRY A. WAXMAN, CALIFORNIA  
EDWARD J. MARKEY, MASSACHUSETTS  
RICK BOUCHER, VIRGINIA  
EDOLPHUS TOWNS, NEW YORK  
FRANK PALLONE, Jr., NEW JERSEY  
BART GORDON, TENNESSEE  
BOBBY L. RUSH, ILLINOIS  
ANNA G. ESHOO, CALIFORNIA  
BART STUPAK, MICHIGAN  
ELIOT L. ENGEL, NEW YORK  
ALBERT R. WYNN, MARYLAND  
GENE GREEN, TEXAS  
DIANA DEGETTE, COLORADO  
VICE CHAIRMAN  
LOIS CAPPS, CALIFORNIA  
MIKE DOYLE, PENNSYLVANIA  
JANE HARMAN, CALIFORNIA  
TOM ALLEN, MAINE  
JAN SCHAKOWSKY, ILLINOIS  
HILDA L. SOLIS, CALIFORNIA  
CHARLES A. GONZALEZ, TEXAS  
JAY INSLEE, WASHINGTON  
TAMMY BALDWIN, WISCONSIN  
MIKE ROSS, ARKANSAS  
DARLENE HOOLEY, OREGON  
ANTHONY D. WEINER, NEW YORK  
JIM MATHESON, UTAH  
G.K. BUTTERFIELD, NORTH CAROLINA  
CHARLIE MELANCON, LOUISIANA  
JOHN BARROW, GEORGIA  
BARON P. HILL, INDIANA

ONE HUNDRED TENTH CONGRESS

**U.S. House of Representatives**  
**Committee on Energy and Commerce**  
**Washington, DC 20515-6115**

JOHN D. DINGELL, MICHIGAN  
CHAIRMAN

JOE BARTON, TEXAS  
RANKING MEMBER  
RALPH M. HALL, TEXAS  
FRED UPTON, MICHIGAN  
CLIFF STEARNS, FLORIDA  
NATHAN DEAL, GEORGIA  
ED WHITFIELD, KENTUCKY  
BARBARA CUBIN, WYOMING  
JOHN SHIMKUS, ILLINOIS  
HEATHER WILSON, NEW MEXICO  
JOHN B. SHADEGG, ARIZONA  
CHARLES W. "CHIP" PICKERING, MISSISSIPPI  
VITO FOSSELLA, NEW YORK  
ROY BLUNT, MISSOURI  
STEVE BUYER, INDIANA  
GEORGE RADANOVICH, CALIFORNIA  
JOSEPH R. PITTS, PENNSYLVANIA  
MARY BONO MACK, CALIFORNIA  
GREG WALDEN, OREGON  
LEE TERRY, NEBRASKA  
MIKE FERGUSON, NEW JERSEY  
MIKE ROGERS, MICHIGAN  
SUE MYRICK, NORTH CAROLINA  
JOHN SULLIVAN, OKLAHOMA  
TIM MURPHY, PENNSYLVANIA  
MICHAEL C. BURGESS, TEXAS  
MARSHA BLACKBURN, TENNESSEE

January 31, 2008

DENNIS B. FITZGIBBONS, CHIEF OF STAFF  
GREGG A. ROTHSCHILD, CHIEF COUNSEL

The Honorable Henry M. Paulson  
Secretary  
U.S. Department of the Treasury  
1500 Pennsylvania Ave., NW  
Washington, D.C. 20220

Dear Mr. Secretary:

As you are well aware, there is growing apprehension in the Congress about the proposed acquisition by Huawei Technologies and its U.S. partner, Bain Capital, LLC, of 3Com Corporation. A number of our colleagues, including Reps. Thaddeus McCotter and Ilena Ros-Lehtinen, have introduced a resolution (H.Res. 730) that details their concerns about this transaction. Given that 3Com Corporation manufactures communications network components – some of which it supplies to the Pentagon, including firewall technology – this transaction raises significant concerns about its potential effect on the national security of the United States. We would stress additionally that our interest in this matter is bipartisan and represents genuine concern for the security of critical U.S. communications infrastructure.

We believe these concerns are more than justifiable, especially in light of recent increases in attacks on government and private networks, as reported in a January 28, 2008, article in The Wall Street Journal. This alarming trend follows allegations, first reported by The Financial Times on September 3, 2007, that the Chinese military hacked into the Pentagon's computer network in 2007. (See attached articles.)

Therefore, pursuant to this Committee's Rule X jurisdiction over foreign and interstate commerce generally, the regulation of interstate and foreign communications, and, most importantly, cybersecurity, we are opening an inquiry into this matter. To assist us in carrying out our responsibilities under the rules of the U.S. House of Representatives, we request responses to the following questions regarding the findings of the Committee on Foreign Investment in the United States (CFIUS) in its evaluation of this proposed transaction:


1. What percentage of interest will Huawei Technologies own in 3Com Corporation, as outlined in the proposed acquisition? If this percentage represents a minority stake, will Huawei Technologies be granted minority investor protections, such as the authority to appoint members to 3Com Corporation's board of directors?
2. What has CFIUS learned about the internal structure and governance of Huawei Technologies? Specifically, who (e.g., shareholders) controls the company? Additionally, who (e.g., board of directors) directs the company's operations? Is this information transparent and easily obtainable?
3. Please describe the extent and nature of Huawei Technologies' ties to the Chinese People's Liberation Army (PLA). Do such ties constitute a threat to U.S. national security? If CFIUS does not believe this, please provide a detailed explanation.
4. Under the terms of the proposed acquisition, will Huawei Technologies be permitted to enter into a technology-sharing agreement with 3Com Corporation? If so, are there any limitations to the agreement, particularly for technologies relevant to protecting the national security of the United States, and a means to ensure compliance with any limitations of the agreement?
5. In the event that this merger is approved, will 3Com Corporation be required to divest itself of subsidiaries that provide critical network infrastructure components to the U.S. Government?


We understand the sensitive nature of the answers to these questions and therefore request that they be given to Committee staff under the auspices of a non-public briefing, preferably to be held no later than Friday, February 28, 2008. To schedule this briefing, please have your staff contact Andrew Woelfling with the Committee on Energy and Commerce staff at (202) 225-2927. Your assistance with this request is appreciated.

Sincerely,

  
\_\_\_\_\_  
John D. Dingell  
Chairman

  
\_\_\_\_\_  
Joe Barton  
Ranking Member

  
\_\_\_\_\_  
Bobby L. Rush  
Chairman  
Subcommittee on Commerce, Trade,  
and Consumer Protection

  
\_\_\_\_\_  
Ed Whitfield  
Ranking Member  
Subcommittee on Commerce, Trade,  
and Consumer Protection

## Chinese military hacked into Pentagon

[Print](#)

By Demetri Sevastopulo in Washington and Richard McGregor in Beijing  
Published: Sep 03, 2007

The Chinese military hacked into a Pentagon computer network earlier this year in the most successful cyber attack ever on the US defence department, according to US officials.

The Pentagon acknowledged shutting down part of a computer system serving the office of Robert Gates, the defence secretary, in June, but refused to say who it believed had been behind the incursion.

Current and former officials have now told the Financial Times that an internal investigation into the attack has revealed it came from the Peoples' Liberation Army.

One senior US official said the Pentagon had pinpointed the exact origins of the attack. Another person familiar with the event said there was a "very high level of confidence ... trending towards total certainty " that the PLA was responsible.

The Defence Ministry in Beijing declined to comment on Monday.

Angela Merkel, Germany's chancellor, raised reports of Chinese infiltration of German government computers with China's premier, Wen Jiabao, in a recent visit to Beijing, after which the Chinese foreign ministry said the government opposed and forbade "any criminal acts undermining computer systems, including hacking ".

"We have explicit laws and regulations in this regard, " said spokeswoman, Jiang Yu, "Hacking is an global issue and China is frequently a victim. "

President George W. Bush is due to meet Hu Jintao, the Chinese president, on Thursday in Australia ahead of the Asia Pacific Economic Co-operation summit.

Cyberspace has emerged as a new theatre of conflict for governments around the increasingly networked world. Earlier this year, for instance, Estonia accused Russia of orchestrating a massive attack that temporarily crippled government networks, a claim Russia denied.

The PLA regularly probes US military networks - and the Pentagon is widely assumed to scan Chinese networks - but officials say the June penetration raised US concerns to a new level because of fears that China has demonstrated the ability to disrupt US systems at critical times.

"The PLA has demonstrated the ability to conduct attacks that disable our system ... and the ability in a conflict situation to re-enter and disrupt on a very large scale, " said a former official, who added that the PLA has also penetrated the networks of US defence companies and think-tanks.

Hackers from multiple locations in China spent several months probing the Pentagon system before they finally overcame its defences, according to people familiar with the matter. The Pentagon took the network down for more than a week to protect it while the attacks continued, and to conduct a comprehensive diagnosis.

"These are multiple wake up calls stirring us to levels of more aggressive vigilance, " said Richard Lawless, the Pentagon's top Asia official at the time of the attacks.

The Pentagon is still investigating how much data was downloaded, but one person with knowledge of the attack said most of the information was probably "unclassified ". He said the event had forced officials to reconsider the kind of information they send over unsecured emails systems.

John Hamre, a Clinton-era deputy defence secretary involved with cyber security, said while he had no knowledge of the June attack, criminal groups sometimes mask cyber attacks to make it appear they came from government computers in a particular country.

Gordon Johndroe, spokesman for the National Security Council, said the White House recently created a team of experts to consider whether the administration needs to restrict the use of Blackberries because of concerns about cyber espionage.

Copyright The Financial Times Limited 2008

"FT" and "Financial Times" are trademarks of the Financial Times. [Privacy policy](#) | [Terms](#)  
© Copyright The Financial Times Ltd 2008.


 FORMAT FOR  
PRINTING  
sponsored by


January 28, 2008

## Bush Looks to Beef Up Protection Against Cyberattacks

**Estimated Cost  
Could Be \$6 Billion;  
Democrats Are Wary**

**By SIOBHAN GORMAN**  
*January 28, 2008; Page A8*

WASHINGTON -- President Bush has promised a frugal budget proposal next month, but one big-ticket item is stirring controversy: an estimated \$6 billion to build a secretive system protecting U.S. communication networks from attacks by terrorists, spies and hackers.

Administration officials and lawmakers say that the prospect of cyberterrorists hacking into a nuclear-power plant or paralyzing Wall Street is becoming possible, and that the U.S. isn't prepared. This is "one area where we have significant work to do," Homeland Security Secretary Michael Chertoff said in a recent interview.

The White House's proposal has already dismayed lawmakers concerned about civil-liberties violations. Democratic lawmakers are also frustrated by what they see as the White House's refusal to provide details of the program, and say that could threaten the fate of the initiative.

Protecting private computer systems would likely require the government to install sensors on private, company networks, officials familiar with the initiative said. Amid divisiveness about other government-surveillance programs, having the government monitor Internet traffic, even in the name of national security, will be a hard sell to Congress and the public.

Cybersecurity specialists say the threat ranges from terrorists hacking into nuclear-power control systems, banks or subways, to foreign governments secretly implanting software to siphon off Pentagon secrets from the government and military contractors.

Last week, a Central Intelligence Agency analyst reported that cyberattacks have disrupted power equipment in unspecified regions outside the U.S. In at least one case, he said, the attack knocked out power in multiple cities. The outages were followed with extortion demands.

### Rising Threat

Homeland Security began tallying standardized data on reported cyber attacks in 2005.	40,000 attacks
	30,000
	20,000



The U.S. government has been monitoring cyberattacks on U.S. systems under a program with the moniker Byzantine Hades. It has tracked, among other threats, continuing operations from China against U.S. computer systems, according to former intelligence officials. They say the program has discovered what appear to be efforts from

### DOW JONES REPRINTS

◀R▶ This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit: [www.djreprints.com](http://www.djreprints.com).

- See a sample reprint in PDF format.
- Order a reprint of this article now.

China to collect information on specific types of U.S. military programs, such as "quiet drive" technology that helps submarines evade detection. Some U.S. officials believe such espionage is connected to the Chinese government.

Homeland Security counted 37,258 attacks on government and private networks last year, compared with 4,095 in 2005, the first year it started counting standardized data.

The administration's plan is to reduce points of access between the Internet and the government and to use sensors to detect intrusions displaying potentially nefarious patterns, said former top intelligence officials. The program would first be used on government networks and then adapted to private networks. Former officials said the final price tag is approaching an estimated \$30 billion over seven years, including a 2009 infusion of around \$6 billion, though those numbers could change significantly as the plan develops.

Access to private networks will be a major sticking point because intelligence agencies, including the National Security Agency, are to play prominent roles.

"We need to be very careful," Mr. Chertoff said. "There is a lot of thought being given to: How do you organize this in a way that protects an incredibly valuable asset in the United States but does it in a way that doesn't alarm reasonable people, and I underline reasonable people, in terms of civil liberties?"

House Homeland Security Committee Chairman Bennie G. Thompson, a Mississippi Democrat, wants the administration to put the program on hold until it can answer congressional concerns. "We don't want to unconstitutionally infringe on the rights of private business under the guise of this new program," Mr. Thompson said.

He said he was particularly irked to learn that Mr. Bush had signed a classified directive that outlines how the White House proposes to bolster security of government networks weeks ago but "has refused to share [the directive] with Congress."

White House spokesman Scott Stanzel said the White House is giving "careful consideration" to Mr. Thompson's request for the Jan. 8 directive, which he described as "a continuation of our efforts to secure government networks, protect against constant intrusion attempts, address vulnerabilities and anticipate future threats."

The structure of the initiative has also been under debate. Officials in Director of National Intelligence Mike McConnell's office argued for a centralized approach, according to a former senior government official. But they appear to have lost the fight in favor of a structure that would dole out responsibilities, and slices of the budget, to individual agencies, two former officials said.

The CIA and the Pentagon didn't want other agencies mucking about in their computer networks; other agencies sought to maintain exclusive relationships with certain industries. Some security experts warn a dispersed structure will invite bureaucratic turf wars. Mr. McConnell's office declined repeated requests for an interview.

Current and former officials said the effort could be scaled back to primarily protect government networks. They would then do what is possible to help the private sector improve its security. Mr. McConnell has said 95% of the problem lies with the private sector.

**Write to Siobhan Gorman** at [siobhan.gorman@wsj.com](mailto:siobhan.gorman@wsj.com)<sup>1</sup>

**URL for this article:**

<http://online.wsj.com/article/SB120147963641320851.html>

**Hyperlinks in this Article:**

(1) <mailto:siobhan.gorman@wsj.com>

**Copyright 2008 Dow Jones & Company, Inc. All Rights Reserved**

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our **Subscriber Agreement** and by copyright law. For non-personal use or to order multiple copies, please contact **Dow Jones Reprints** at 1-800-843-0008 or visit [www.djreprints.com](http://www.djreprints.com).

**RELATED ARTICLES AND BLOGS**

**Blog Posts About This Topic**

- [Bush Order Expands Network Monitoring](#) [roguegovernment.com](http://roguegovernment.com)
- [The Westerner](#) [thewesterner.blogspot.com](http://thewesterner.blogspot.com)

**More related content** *Powered by Sphere* 