COMMITTEES:
ARMED SERVICES
SUBCOMMITTEE ON
READINESS – RANKING MEMBER

SUBCOMMITTEE ON
SEAPOWER AND EXPEDITIONARY FORCES

JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY

SUBCOMMITTEE ON
COMMERCIAL AND ADMINISTRATIVE LAW

J. Randy Forbes
United States Congress
4th District, Virginia

2438 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-6365

425-H SOUTH MAIN STREET
EMPORIA, VA 23847
(434) 634-5575

2903 BOULEVARD, SUITE B
COLONIAL HEIGHTS, VA 23834
(804) 526-4969

505 INDEPENDENCE PARKWAY
LAKE CENTER II – SUITE 104
CHESAPEAKE, VA 23320
(757) 382-0080

April 9, 2010

The Honorable Ike Skelton
Chairman, House Committee on Armed Services
2120 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Skelton:

Cyber-warfare has skyrocketed to prominence as a critical threat to the U.S. Department of Defense's military operations by threatening the exclusivity and security of our cyber-networks.

Of particular concern is the direct threat that China poses to our cyber-security. China has been the point of origin for a barrage of malicious and damaging cyber attacks targeting defense-related information. For example, in 2007, the Office of the Secretary of Defense was compelled to shut down its computer information systems for more than one week in order to defend against infiltration attempts that were found to be coming from China. The Department of Defense experienced roughly 44,000 cyber-warfare attacks from China in the first six months of 2009 alone, resulting in expenditures of more than $100 million to repair the damage from such attacks. In April 2009, reports surfaced that sophisticated attacks on defense contractor systems in 2007 and 2008 allowed intruders to obtain sensitive data related to the design and electronics systems of one of the United States' most advanced fighter planes, the F-35 Joint Strike Fighter.

The realization of the severe consequences of successful cyber attacks is beginning to set in. On May 29th, 2009, President Obama labeled cyber attacks "one of the most serious economic and national security challenges" that the country faces. In June 2009, Secretary of Defense Robert Gates established the U.S. Cyber Command to coordinate a computer-network defense. On January 21, 2010, Deputy Secretary of Defense William Lynn said that "[i]f we don't maintain our capabilities to defend our networks in the face of an attack, the consequences for our military -- and indeed, for our whole national security -- could be dire."

As your Committee begins to prepare the fiscal year 2011 National Defense Authorization Act, please consider this letter as a request for the House Committee on Armed Services to convene a hearing to examine the impact of the cyber-warfare threat to our military readiness and to ensure Members have the opportunity to hear from expert witnesses on this growing threat to the defense of the United States.

Please contact me or Sam Riser from my staff at (202) 225-6365 / Sam.Riser@mail.house.gov with any questions regarding this request. Thank you in advance for your consideration. With kind personal regards, I am

Sincerely,

J. Randy Forbes
Member of Congress

JRF:str