

## Computer Spies Breach Fighter-Jet Project

By SIOBHAN GORMAN, AUGUST COLE and YOCHI DREAZEN

WASHINGTON -- Computer spies have broken into the Pentagon's \$300 billion Joint Strike Fighter project -- the Defense Department's costliest weapons program ever -- according to current and former government officials familiar with the attacks.

Similar incidents have also breached the Air Force's air-traffic-control system in recent months, these people say. In the case of the fighter-jet program, the intruders were able to copy and siphon off several terabytes of data related to design and electronics systems, officials say, potentially making it easier to defend against the craft.

The latest intrusions provide new evidence that a battle is heating up between the U.S. and potential adversaries over the data networks that tie the world together. The revelations follow a recent Wall Street Journal report that computers used to control the U.S. electrical-distribution system, as well as other infrastructure, have also been infiltrated by spies abroad.

Attacks like these -- or U.S. awareness of them -- appear to have escalated in the past six months, said one former official briefed on the matter. "There's never been anything like it," this person said, adding that other military and civilian agencies as well as private companies are affected. "It's everything that keeps this country going."

Many details couldn't be learned, including the specific identity of the attackers, and the scope of the damage to the U.S. defense program, either in financial or security terms. In addition, while the spies were able to download sizable amounts of data related to the jet-fighter, they weren't able to access the most sensitive material, which is stored on computers not connected to the Internet.

Former U.S. officials say the attacks appear to have originated in China. However it can be extremely difficult to determine the true origin because it is easy to mask identities online.

A Pentagon report issued last month said that the Chinese military has made "steady progress" in developing online-warfare techniques. China hopes its computer skills can help it compensate for an underdeveloped military, the report said.

The Chinese Embassy said in a statement that China "opposes and forbids all forms of cyber crimes." It called the Pentagon's report "a product of the Cold War mentality" and said the allegations of cyber espionage are "intentionally fabricated to fan up China threat sensations."

The U.S. has no single government or military office responsible for cyber security. The Obama administration is likely to soon propose creating a senior White House computer-security post to coordinate policy and a new military command that would take the lead in protecting key computer networks from intrusions, according to senior officials.

The Bush administration planned to spend about \$17 billion over several years on a new online-security initiative and the Obama administration has indicated it could expand on that. Spending on this scale would represent a potential windfall for government agencies and private contractors at a time of falling budgets. While specialists broadly agree that the threat is growing, there is debate about how much to spend in defending against attacks.

The Joint Strike Fighter, also known as the F-35 Lightning II, is the costliest and most technically challenging weapons program the Pentagon has ever attempted. The plane, led by [Lockheed Martin Corp.](#), relies on 7.5 million lines of computer code, which the Government Accountability Office said is more than triple the amount used in the current top Air Force fighter.

Six current and former officials familiar with the matter confirmed that the fighter program had been repeatedly broken into. The Air Force has launched an investigation.

Pentagon officials declined to comment directly on the Joint Strike Fighter compromises. Pentagon systems "are probed daily," said Air Force Lt. Col. Eric Butterbaugh, a Pentagon spokesman. "We aggressively monitor our networks for intrusions and have appropriate procedures to address these threats." U.S. counterintelligence chief Joel Brenner, speaking earlier this month to a business audience in Austin, Texas, warned that fighter-jet programs have been compromised.

Foreign allies are helping develop the aircraft, which opens up other avenues of attack for spies online. At least one breach appears to have occurred in Turkey and another country that is a U.S. ally, according to people familiar with the matter.

Joint Strike Fighter test aircraft are already flying, and money to build the jet is included in the Pentagon's budget for this year and next.

Computer systems involved with the program appear to have been infiltrated at least as far back as 2007, according to people familiar with the matter. Evidence of penetrations continued to be discovered at least into 2008. The intruders appear to have been interested in data about the design of the plane, its performance statistics and its electronic systems, former officials said.

The intruders compromised the system responsible for diagnosing a plane's maintenance problems during flight, according to officials familiar with the matter. However, the plane's most vital systems -- such as flight controls and sensors -- are physically isolated from the publicly accessible Internet, they said.

The intruders entered through vulnerabilities in the networks of two or three contractors helping to build the high-tech fighter jet, according to people who have been briefed on the matter. Lockheed Martin is the lead contractor on the program, and [Northrop Grumman Corp.](#) and [BAE Systems PLC](#) also play major roles in its development.

Lockheed Martin and BAE declined to comment. Northrop referred questions to Lockheed.

The spies inserted technology that encrypts the data as it's being stolen; as a result, investigators can't tell exactly what data has been taken. A former Pentagon official said the military carried out a thorough cleanup.

Fighting online attacks like these is particularly difficult because defense contractors may have uneven network security, but the Pentagon is reliant on them to perform sensitive work. In the past year, the Pentagon has stepped up efforts to work with contractors to improve computer security.

Investigators traced the penetrations back with a "high level of certainty" to known Chinese Internet protocol, or IP, addresses and digital fingerprints that had been used for attacks in the past, said a person briefed on the matter.

As for the intrusion into the Air Force's air-traffic control systems, three current and former officials familiar with the incident said it occurred in recent months. It alarmed U.S. national security officials, particularly at the National Security Agency, because the access the spies gained could have allowed them to interfere with the system, said one former official. The danger is that intruders might find weaknesses that could be exploited to confuse or damage U.S. military craft.

Military officials declined to comment on the incident.

In his speech in Austin, Mr. Brenner, the U.S. counterintelligence chief, issued a veiled warning about threats to air traffic in the context of Chinese infiltration of U.S. networks. He spoke of his concerns about the vulnerability of U.S. air traffic control systems to cyber infiltration, adding "our networks are being mapped." He went on to warn of a potential situation where "a fighter pilot can't trust his radar."

**Write to** Siobhan Gorman at [siobhan.gorman@wsj.com](mailto:siobhan.gorman@wsj.com), August Cole at [august.cole@dowjones.com](mailto:august.cole@dowjones.com) and Yochi Dreazen at [yochi.dreazen@wsj.com](mailto:yochi.dreazen@wsj.com)

Printed in The Wall Street Journal, page A1

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)