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.

By Siobhan Gorman, August Cole and Yochi Dreazen

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 sizeable amounts of data related to the fighter-jet, 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 cybercrime.” 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 $7.7 billion over several years on a new online-security initiative and the Obama administration has indicated it plans to ramp up its efforts. Please turn to page A2.