which should advance U.S. national security interests while flagging any legal, ethical, and strategic implications of emerging UAV-related technologies. ***IAJ***

Report Addresses Cyber, Terror Threats

The Bipartisan Policy Center released a report in July warning of myriad cybersecurity and terrorism threats to the United States. The report, *Today's Rising Terrorist Threat and the Danger to the United States: Reflections on the Tenth Anniversary of The 9/11 Commission Report*, is a product of former 9/11 Commissioners.

According to the commissioners, the U.S. fight against terrorism has entered "a new and dangerous phase," with Al Qaeda-affiliated groups gaining strength throughout the Middle East. The report also cites foreign fighters returning from Syria and Iraq, resistance to counterterrorism reform among members of Congress, and "counterterrorism fatigue" among U.S. citizens as growing concerns. On the cyber front, the commissioners assert that cyber readiness lags far behind the threat, saying that the U.S. is "at September 10th levels in terms of cyber preparedness."

Proactive counterterrorism measures are needed to deter these threats, and the commissioners make many recommendations in this report. Included in their recommendations are the sustainment of counterterrorism authorities and budgets, increased transparency with the American public, and Congressional legislation to address and counter cyber threats.

The commissioners also recommend that future Directors of National Intelligence should focus on coordinating the efforts of the various intelligence agencies and advancing interagency information sharing, especially counterterrorism information sharing throughout the Intelligence Community. ***IAJ***

Cyber Exercise Improves Interagency Cooperation

In July, 550 participants engaged in Cyber Guard 14-1, a two-week exercise designed to test operational and interagency coordination in the event of a domestic cyberspace incident. Participants included elements of the National Guard Reserves, National Security Agency, and U.S. Cyber Command, as well as individuals involved in U.S. government, academia, and industry.

During the exercise, Cyber Guard participants demonstrated their support to Department of Homeland Security (DHS) and FBI responses to foreign-based cyberattacks on simulated critical infrastructure networks. The exercise acted as a "test drive" of operational capabilities and interagency coordination between DoD components, the FBI, and DHS.

Officials stated that in the event of a domestic cyber incident, federal agencies have specific, complementary roles. Greg Touhill, deputy assistant secretary of homeland security for cybersecurity operations and programs, stressed the importance of interagency preparedness, saying that "Practicing as an interagency team is essential to ensure national response to cyber events produce results that are effective and efficient."

The event was executed by Cybercom and hosted by the FBI at the National Academy in Quantico, Virginia. ***IAJ***