Excerpts from the "black budget," Volume 2, "Combined Cryptologic Program":

(U) RESEARCH & TECHNOLOGY (U) PENETRATING HARD TARGETS

(U) Project Description

(S//SI//REL TO USA, FVEY) The Penetrating Hard Targets Project provides proof-of-concept technological solutions to *{...}* enable:

{...}

- (S//SI//REL TO USA, FVEY) Breaking strong encryption.

(TS//SI//REL TO USA, FVEY) This Project focuses on meeting those customer requirements that will directly impact the end-to-end SIGINT mission during the next decade and beyond. It provides advanced knowledge of technology trends and opportunities to steer IT products and standards in a SIGINT-friendly direction. This Project contains the Penetrating Hard Targets Sub-Project.

(U) Base resources in this project are used to:

{...}

- (S//SI//REL TO USA, FVEY) Conduct basic research in quantum physics and architecture/engineering studies to determine if, and how, a cryptologically useful quantum computer can be built.

{...}

(U) The CCP expects this Project to accomplish the following in FY 2013:

{...}

- (TS//SI//REL TO USA, FVEY) Demonstrate dynamical decoupling and complete quantum control on two semiconductor qubits. A qubit is the basic “building block” of a quantum computer. This will enable initial scaling towards large systems in related and follow-on efforts. [CCP_0127]

(U) RESEARCH & TECHNOLOGY

(U) OWNING THE NET

(U) Project Description

(TS//SI//REL TO USA, FVEY) The Owning the Net (OTN) Project provides the technological means for NSA/CSS to gain access to and securely return high value target communications. By concentrating on the means of communication, the network itself, and network links rather than end systems, OTN research manipulates equipment hardware and software to control an adversary's network. Research is conducted at the Laboratory for Telecommunications Sciences in College Park, MD, and supports the evolving NSA/CSS internal information infrastructure and the larger IC.

{...}

(U) Base resources in this project are used to:

{...}

- (TS//SI//REL TO USA, FVEY) Continue research of quantum communications technology to support the development of novel Quantum Key Distribution (QKD) attacks and assess the security of new QKD system designs.