

Building Cyberwarfare Capabilities in Public Documents

- Recent budget justification documents
- Recent contract and proposal solicitations

February 2010

Air Force Cyberwarfare in Budget Documents and Solicitations

SOLICITATION

Dominant Cyber Offensive Engagement and Supporting Technology

BAA-08-04-RIKA

Agency: Department of the Air Force

Office: Air Force Materiel Command

Location: AFRL - Rome Research Site

Posted on fbo.gov: June 13, 2008

“Solutions to basic and applied research and engineering for the problems relating to Dominant Cyber Offensive Engagement and Supporting Technology are sought. This includes high risk, high payoff capabilities for gaining access to any remotely located open or closed computer information systems; these systems enabling full control of a network for the purposes of information gathering and effects based operations”

“Also, we are interested in technology to provide the capability to maintain an active presence within the adversaries' information infrastructure completely undetected. Of interest are any and all techniques to enable stealth and persistence capabilities on an adversaries infrastructure. This could be a combination of hardware and/or software focused development efforts. Following this, it is desired to have the capability to stealthily exfiltrate information from any remotely-located open or closed computer information systems with the possibility to discover information with previously unknown existence. Any and all techniques to enable exfiltration techniques on both fixed and mobile computing platforms are of interest. Consideration should be given to maintaining a "low and slow" gathering paradigm in these development efforts to enable stealthy operation. Finally, this BAA's objective includes the capability to provide a variety of techniques and technologies to be able to affect computer information systems through Deceive, Deny, Disrupt, Degrade, Destroy (D5) effects.”

Air Force Cyberwarfare in Budget Documents and Solicitations

PE 0602788F: Dominant Information Technology

- “MAJOR THRUST: Develop offensive cyber operations technologies to access, maintain presence on, and deliver effects to adversary systems.
- FY 2010 Plans: “Continue development of information system access methods and development of propagation techniques. Continue development of stealth and persistence technologies. Initiate development of the capability to exfiltrate information from adversary information systems for generation of actionable CybINT. Continue technology development for preparation of the battlefield and increased situational awareness and understanding. Continue development of technology to deliver D5 (deceive, deny, disrupt, degrade, and destroy) effects. Initiate efforts to develop autonomic technologies for operating within adversary information systems. Initiate development of techniques for covert communication among agents operating within adversary information systems. Initiate analysis of proprietary hardware and software systems to identify viable means of access and sustained operations within the same. Initiate efforts to develop a pub/sub architecture for exchange and exfiltration of information while operating within adversary information systems. Demonstrate ability to identify foreign languages as a part of a CybINT capability.”
- FY 2011 Base Plans: “Continue development of information system access methods and development of propagation techniques. Continue development of stealth and persistence technologies. Continue development of the capability to exfiltrate information from adversary information systems for generation of actionable CybINT. Continue technology development for preparation of the battlefield and increased situational awareness and understanding. Continue development of technology to deliver D5 effects. Continue development of autonomic technologies for operating within adversary information systems. Continue development of techniques for covert communication among agents operating within adversary information systems. Continue analysis of proprietary hardware and software systems to identify viable means of access and sustained operations within the same. Continue development of a publish/subscribe architecture for exchange and exfiltration of information while operating within adversary information systems. Initiate development of techniques to deliver PsyOps via cyber channels. Develop deception techniques to allow misdirection and confusion of adversary attempts to probe and infiltrate AF systems.”

DOD Fiscal Year (FY) 2011 President’s Budget. Air Force: Justification Book Volume 1. Research, Development, Test and Evaluation, Air Force. Released February 2010.

Air Force Cyberwarfare in Budget Documents and Solicitations

PE 0603788F: Global Information Dev/Demo

- “MAJOR THRUST: Develop and demonstrate offensive cyber operations capabilities in a series of Experimental Cyber Craft technology demonstrations.
- FY 2010 Plans: “Continue to analyze development of additional offensive cyber operations capabilities, integrated kinetic and cyber operations planning and execution capabilities, and cyber command and control (Cyber C2) operations functions. Complete selected offensive cyber capabilities to access, remain stealthy, gather intelligence, and affect adversary information and information systems. Finalize technology demonstration plans.”
- FY 2011 Base Plans: “Continue to analyze development of additional offensive cyber operations capabilities, integrated kinetic and cyber operations planning and execution capabilities, and Cyber C2 operations functions.”

DOD Fiscal Year (FY) 2011 President’s Budget. Air Force: Justification Book Volume 1. Research, Development, Test and Evaluation, Air Force. Released February 2010.

Air Force Cyberwarfare in Budget Documents and Solicitations

PE 0603788F: Global Information Dev/Demo

- “MAJOR THRUST: Develop and demonstrate offensive cyber operations capabilities in a series of Experimental Cyber Craft technology demonstrations. These demonstrations will integrate capabilities developed from ongoing offensive cyber programs in the areas of gaining access to systems, performing operations in a stealthy manner, gathering intelligence from the compromised systems and launching cyber "effects" against the systems. Note: Prior to FY 2010, efforts were conducted in PE 0603789F, Project 4216...”
- In FY 2010 “Continue to analyze development of additional offensive cyber operations capabilities, integrated kinetic and cyber operations planning and execution capabilities, and cyber command and control (Cyber C2) operations functions. Complete selected offensive cyber capabilities to access, remain stealthy, gather intelligence, and affect adversary information and information systems. Finalize technology demonstration plans.”

Department of the Air Force Fiscal Year 2010 Budget Estimates. Research, Development, Test and Evaluation. Descriptive Summaries, Volume I. Released May 2009.

Air Force Cyberwarfare in Budget Documents and Solicitations

PE 0603789F: C3I Advanced Development

- “It will also demonstrate offensive cyber operations technologies allowing attack and exploitation of adversary information systems by the Air Force.”
- “MAJOR THRUST: Develop and demonstrate offensive cyber operations capabilities in a series of experimental cyber craft technology demonstrations. These demonstrations will integrate capabilities developed from ongoing offensive cyber programs in the areas of gaining access to systems, performing operations in a stealthy manner, gathering intelligence from the compromised systems, and launching cyber "effects" against the systems...”
- In FY 2008: “Initiated development of offensive cyber capabilities to access, remain stealthy, gather intelligence, and affect adversary information and information systems. Developed technology demonstration plans for cyber operations.”
- In FY 2009: “Analyze development of selected offensive cyber operations capabilities, integrated kinetic and cyber operations planning and execution capabilities, and cyber command and control (Cyber C2) operations functions.”

Department of the Air Force Fiscal Year 2010 Budget Estimates. Research, Development, Test and Evaluation. Descriptive Summaries, Volume I. Released May 2009.

Air Force Cyberwarfare in Budget Documents and Solicitations

SOLICITATION

Cyber Defensive & Offensive Operations Technology (CDOT)

BAA-03-18-IFKA

Agency: Department of the Air Force

Office: Air Force Materiel Command

Location: AFRL - Rome Research Site

Posted on fbo.gov: December 11, 2003

“The technologies being pursued will provide greater functions and capabilities within the Information Warfare domain and push not only Air Force and DoD needs, but also those of National Security, Homeland Defense and Critical Infrastructure Protection...”

“A. Covert Cyber Operations. The area of Covert Cyber Operations holds tremendous potential as a major future thrust for AFRL/IF. It is an area that can be described as allowing us access to the cyberspace domain for the purpose of adversary monitoring, intelligence gathering or information-based attack. In order to make the Covert Cyber Operations area a fully functional Air Force capability we must develop effects-based tools that allow us to plan for and achieve the desired effects of a planned cyber operation. For example, deploying effects-based tools that give decision makers lines of reasoning and their respective scenario implications would be valuable addition to the Cyber Operations and conventional warfare arsenal. This gives the decision maker a comprehensive "information set" that presents only useful information and disallows noise. Work is needed in the areas of Cyber ISR and Computer Network Attack (CNA). Cyber ISR entails developing technology for gathering information about the adversary, their intentions, and their capabilities and is necessary for identification and targeting of the adversary in cyberspace. CNA tools and systems that must be developed to penetrate an adversary's detection system and remain hidden until triggered. Cyber Operations interest areas include access, targeting, mission planning, attack effectiveness measures, attack damage assessment, and CNA tool development.”

“A focus for future designs is Biologically Inspired Cyber Operations area. It is an area that holds promise for ... even carrying out computer network attacks against an adversary...”

Army Cyberwarfare in Budget Documents and Solicitations

PE 0303028A: Security & Intel Activities

- “INSCOM's [United States Army Intelligence and Security Command's] RDTE program provides the Army with low-density, high-demand, extremely advanced offensive cyberspacetechnologies [sic] designed to degrade, deny, disrupt, or destroy adversary C4I and shape the operational warfighting environment in order to create conditions favorable to the application of other elements of national power.”

Supporting Data FY 2011 Budget Estimate Submitted to OSD – February 2010. Descriptive Summaries of the Research, Development, Test and Evaluation Army Appropriation, Budget Activity 7. Department of the Army, Office of the Secretary of the Army (Financial Management and Comptroller).

Additional Budget Document and Solicitation Language

Army Cyberwarfare in Budget Documents and Solicitations

PE 0602270A: Electronic Warfare Technology

- “Offensive Information Operations Technologies: This effort investigates and develops techniques that identify and capture data traversing targeted networks for the purpose of Information Operations or otherwise countering adversary communications.”
- In FY10, “define distributed communications to allow the technologies to communicate and migrate between nodes; begin development of interception and countermeasure capabilities against network traffic flows of interest; develop Network Operations techniques against relevant high priority protocols; research methods to link this Computer Network Operations (CNO) framework to previously developed Electronic Warfare (EW) frameworks.”
- In FY11, “will develop capability for identification and capture of protocols of interest; will implement algorithms to allow for surgical and coordinated exploitation amongst nodes; will develop traffic analysis techniques to discriminate amongst individual data sessions; will prototype communication and coordination capabilities between CNO and EW systems.”

Supporting Data FY 2011 Budget Estimate Submitted to OSD – February 2010. Descriptive Summaries of the Research, Development, Test and Evaluation Army Appropriation, Budget Activity 2. Department of the Army, Office of the Secretary of the Army (Financial Management and Comptroller).

Navy Cyberwarfare in Budget Documents and Solicitations

PE 0204575N: Elect Warfare Readiness Supt

- “The Navy Offensive Cyber and Information Warfare Program (NOCIWP) discovers adversary vulnerabilities, develops capabilities to exploit these vulnerabilities, and transitions these capabilities for operational use. Investments are made in high risk/high payoff non kinetic opportunities and result in technologies and capabilities that provide unique, innovative, life-saving, and potentially cost saving applications into Department of Navy and Department of Defense classified acquisition and intelligence programs. Measures include quality and impact of new ideas and approaches, the success of the technology application in satisfying COCOM and Fleet requirements, and successful cost effective transition of the capability into operational systems. The goal of these investments is to provide to Commanders non kinetic options to influence adversaries and prevent escalation of crises. Due to the nature and classification of these efforts qualitative measures are used. It is the intent through the development of modeling and simulation scenarios and capabilities to develop quantitative metrics. The success of this depends heavily on the insight obtained via various intelligence community efforts.”

Department of the Navy Fiscal Year 2011 Budget Estimates. Justification of Estimates February 2010. Research, Development, Test and Evaluation, Navy. Budget Activity 7.

Navy Cyberwarfare in Budget Documents and Solicitations

SOLICITATION

Cyber Warfare Support

SSC-Pacific_MKTSVY_6F32A

Agency: Department of the Navy

Office: Space and Naval Warfare Systems Command

Location: SPAWAR Systems Center San Diego

Posted on fbo.gov: February 24, 2009 [Available online, but still labeled FOUO]

“Increasingly, SSC PAC DoD and other government customers require advice, assistance, coordination and products to support the operational planning and execution and technology development required to assure superiority for the warfighter in the Cyberspace domain. A subset of the activities, both offensive and defensive, required to achieve superiority in Cyberspace are those that fall into the Information, Influence and Cyber Operations disciplines”

“The scope of this contract will include efforts to examine the architecture, engineering, functionality, interface and interoperability of Cyber Warfare collection, surveillance, exploitation and attack systems at the tactical and National levels, to include all enabling technologies.”

Air Force Cyberwarfare in Budget Documents and Solicitations

PE 0602788F: Dominant Information Technology

- “the Air Force requires technologies to deliver a full range of options in cyberspace at par with air and space dominance in each of the areas of cyber attack, cyber defense, and cyber support to achieve the strategic capability of cyber dominance.”
- “MAJOR THRUST: Develop offensive cyber operations technologies to access, maintain presence on, and deliver effects to adversary systems. Note: Prior to FY 2010, efforts were conducted in PE 0602702F, Project 4519.”

Department of the Air Force Fiscal Year 2010 Budget Estimates. Research, Development, Test and Evaluation. Descriptive Summaries, Volume I. Released May 2009.

Air Force Cyberwarfare in Budget Documents and Solicitations

SOLICITATION

Information Warfare: Offensive and Defensive Counterinformation

BAA-06-12-IFKA

Agency: Department of the Air Force

Office: Air Force Materiel Command

Location: AFRL - Rome Research Site

Posted on fbo.gov: March 6, 2009

“The objective of this BAA is to address highly innovative R&D areas in information operations. Proposed work should address the innovative and strategic thought of the 21st century adversary, and develop new concepts to counter with innovative information-based capabilities. Further, proposed work should address new concepts for continuously analyzing the information battle space to identify US vulnerabilities and adversary weaknesses, and develop new defensive and offensive strategies and capabilities accordingly.”

“Network Attack: Employment of network-based capabilities to destroy, disrupt, degrade, deny, delay, corrupt or usurp information resident in or transiting through networks. A primary effect is to influence the adversary commander's decisions.”

Air Force Cyberwarfare in Budget Documents and Solicitations

SOLICITATION

AIR FORCE INFORMATION OPERATIONS BATTLELAB OPERATIONAL CONCEPT DEMONSTRATIONS

BAA-AIA-07-0001

Agency: Department of the Air Force

Office: Air Combat Command

Location: AF ISR Agency/A7KA

Posted on fbo.gov: September 27, 2006

This looks to be a follow-on to: FA7037-06-BAA-0001 that was posted on September 30, 2005; FA7037-05-BAA-0001 posted on September 24, 2004; FA7037-04-BAA-0001 that was posted on September 29, 2003; and F41621-03-BAA-0001 posted on September 30, 2002

“This BAA solicits concept papers with the potential to enhance Air Force operations within any element of IO or key technologies that enable IO. These topics include, but are not limited to: “

“(b) Network Warfare Ops: Network warfare operations are the integrated planning and employment of military capabilities to achieve desired effects across the interconnected analog and digital network portion of the battlespace. Network warfare operations are conducted in the information domain through the combination of hardware, software, data, and human interaction. Networks in this context are defined as any collection of systems transmitting information. This includes but is not limited to radio nets; satellite links; tactical digital information links (TADIL); telemetry; digital track files and supervisory control and data acquisition (SCADA) systems; telecommunications; and wireless communications networks and systems.

i. Network Attack (NetA), ii. Network Defense (NetD) , iii. Network Warfare Support (NS).”