

ARCHIVED REPORT

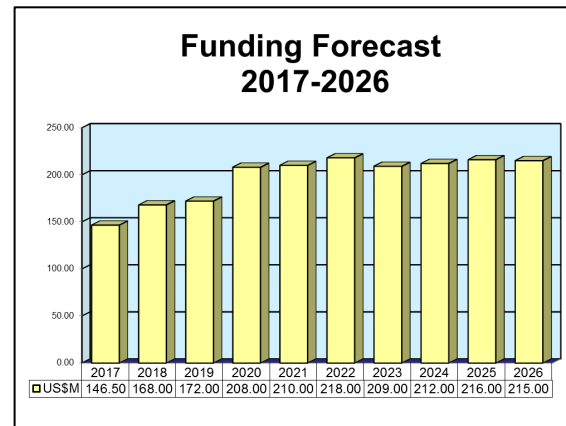
For data and forecasts on current programs please visit

www.forecastinternational.com or call +1 203.426.0800

Network Centric Enabling Technology

Outlook

- Forecast International projects that DARPA will spend about \$1.98 billion on its Network Centric Enabling Technology project over the next decade
- DARPA funding is driven by the U.S. DoD's need to develop technology for network-centric tactical operations
- Expect projected funding to peak in FY22



Orientation

Description. DARPA's Network Centric Enabling Technology project develops applications that integrate information arising from: 1) intelligence networks; 2) open and other external sources; 3) sensors and signal/image processors; and 4) collection platforms and weapon systems.

Status. Ongoing research and development.

Application. Network-centric tactical operations.

Sponsor

U.S. Defense Advanced Research Projects Agency
3701 N Fairfax Dr
Arlington, VA 22203-1714

Contractors

Contractor(s) not selected or not disclosed.

Contractors are invited to submit updated information to Editor, International Contractors, Forecast International, 22 Commerce Road, Newtown, CT 06470, USA; rich.pettibone@forecast1.com

Network Centric Enabling Technology

Technical Data

The Network Centric Enabling Technology project addresses technical challenges that include the need of military commands to process huge volumes of diverse, incomplete, and uncertain data in tactically relevant timeframes. The project's data processing efforts include: the conditioning of unstructured data, content analysis, behavioral modeling, pattern-of-life characterization, economic activity analysis, social network analysis, anomaly detection, and visualization. The project provides a deeper understanding of the evolving operational environment, tailoring technologies to the needs of commanders at every echelon. Promising technologies are evaluated in the laboratory and demonstrated in the field to facilitate transition.

The Network Centric Enabling Technology project is part of PE#0602702E (Tactical Technology), and consists of the following subprojects:

XDATA. The XDATA subproject develops computational techniques and software tools for analyzing large volumes of data, both semi-structured (e.g., tabular, relational, categorical, meta-data, spreadsheets) and unstructured (e.g., text documents, message traffic). This subproject develops scalable algorithms for processing imperfect data in distributed data stores, and designs effective human-computer interaction tools for facilitating rapidly customizable visual reasoning for diverse missions. It will develop open-source software toolkits that support the processing of large volumes of data in timelines commensurate with mission workflows.

An XDATA framework will help minimize the design-to-deployment time of new analytic and visualization technologies.

Network Defense. The Network Defense subproject develops technologies to detect network attacks using network summary data. U.S. computer networks are continually under attack, and these attacks are typically handled by individual organizations as they occur. Analyzing network summary data across a wide array of networks will make it possible to identify trends and patterns visible only when the data is viewed as a whole, and to detect recurring threats, patterns of activity, and persistent vulnerabilities. Network Defense develops novel algorithms and analysis tools that enable a big-picture approach for identifying illicit behavior in networks. This analysis and subsequent feedback to system administrators, security engineers, and decision-makers will enhance information security in both the government and commercial sectors.

Memex. The Memex subproject develops the next generation of search technologies to "revolutionize" the discovery, organization, and presentation of domain-specific content. Current search technologies have limitations in search query format, retrieved content organization, and infrastructure support, and the iterative search process they enable is time-consuming and inefficient, typically finding only a fraction of the available information. Memex creates a new domain-specific search paradigm to discover relevant content and organize it in ways that are more immediately useful to specific missions and tasks.

In addition, Memex domain-specific search engines will extend the reach of current search capabilities to the deep Web and non-traditional content. Memex technologies will enable the military, the government, and commercial enterprises to find and organize mission-critical information on the Internet and in large intelligence repositories. Anticipated mission areas include counterterrorism, counter-drug operations, anti-money-laundering, and anti-human-trafficking. The Memex subproject expands on research originally programmed under the Nexus 7 subproject.

Distributed Battle Management. The Distributed Battle Management subproject develops mission-driven architectures, protocols, and algorithms for battle management in a contested environment. The military is turning to networked weapons and sensors on board a heterogeneous mix of multipurpose manned and unmanned systems. In contested environments, it is a challenge for command and control (C2) networks to communicate with subordinate platforms due to extensive adversarial cyber- and electronic-warfare operations, anti-satellite attacks, and the need for emissions control in the face of a formidable integrated air defense system.

The DBM subproject seeks to develop a distributed command architecture with decentralized control of mission-focused asset teams. The architecture will enable rapid reaction to ephemeral engagement opportunities and maintain a reliable C2 structure, despite limited communications and platform attrition in continuously evolving threat environments. It will incorporate highly automated decision-making capability while maintaining vital human-on-the-loop operator approval.

Quantitative Crisis Response. The Quantitative Crisis Response subproject develops and applies big data analysis and visualization methodologies to better understand the true nature of non-traditional threats; track the effectiveness of remedial measures; and

Network Centric Enabling Technology

develop/optimize alternative strategies. Extremely challenging non-traditional threats have recently arisen, including illicit networks of (human) traffickers and infectious diseases like Ebola. To counter illicit networks, it is important to detect their activities, which often take place on the "dark Web," and to derive their command and control structure. Infectious disease contagion presents a somewhat different challenge – specifically, finding patterns in the spread of the disease and factors that favor/mitigate its propagation. There is also interest in quantitative methods for countering the proliferation of weapons of mass terrorism. QCR will be coordinated with and transitioned to multiple national security agencies.

Media Forensics (MediFor). The Media Forensics (MediFor) subproject will develop technologies for use in analyzing diverse types of content and media to determine how trustworthy they are for military and intelligence purposes. Once developed, the technologies will be transitioned to operational commands and the intelligence community. This program was previously funded in PE#0603767E, Project SEN-03.

Science of Human and Computer Training. The Science of Human and Computer Teaming subproject will develop and demonstrate data-driven approaches for the formation and training of teams comprising humans and computers.

Conventional approaches to military personnel selection, role assignment, and training are optimized for individual performance, but military operations are typically performed by teams, and future teams are likely to also include autonomous systems that use artificial intelligence (AI) to sense, reason, learn, and interact. Behavioral scientists are studying the performance of groups across diverse sets of tasks and developing performance assessment techniques for group work. Interesting early results suggest that groups exhibit a form of intelligence beyond that of the individual members, and that group intelligence has social correlates. Computer scientists are looking at ways in which humans may team with computers to achieve superior levels of performance. Such human-computer teams have shown great promise in highly structured competitive domains such as chess.

Realizing this promise in battlefield environments will require intuitive, low-latency, high-bandwidth, human-computer interfaces that enable computers to be better teammates. The subproject will identify individual characteristics predictive of performance of mixed human-computer teams; develop techniques for measuring these characteristics in military personnel; demonstrate the capability to select human-computer teams and train them to be superior in performance to human-only teams formed and trained using current methods; and develop an understanding of how to structure human-computer teams for military missions such as cyber defense and intelligence analysis.

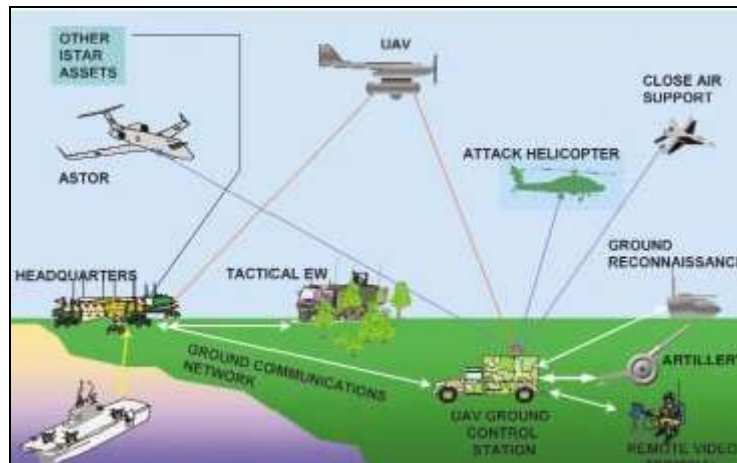
Predicting Complex Operational Environments.

The Predicting Complex Operational Environments subproject expands on work done under the XDATA subproject. It will develop advanced modeling, analysis, simulation, and visualization tools to enable command staffs to rapidly and effectively plan and manage missions in complex operational environments.

The U.S. military increasingly operates in remote and unstable parts of the world where mission success depends heavily on cooperation with and among a wide variety of stakeholder groups. These groups typically include host nation government organizations, local civilian groups, and non-governmental organizations, each of which has individual priorities and concerns. Economic disruptions can add urgency to these considerations, as shortages of water and food directly impact theater security and may even lead to war.

Current mission planning and plan assessment / adaptation technologies do not adequately model the inherent uncertainties. Meeting this challenge will require the creation of new semantic techniques that automatically generate, update, and "prune" alternative hypotheses as they become more likely given incoming data streams. This subproject will create computational models that represent the most significant dynamics and uncertainties of the operational environment, including political, military, economic, and social factors. These will enable command staffs to develop and assess potential courses of action at multiple levels of granularity and time scales, and to quickly adapt to changing situations.

Network Centric Enabling Technology



Network Centric Warfare

Source: Public Domain

Program Review

The following discusses the recent activity in the Network Centric Enabling Technology subprojects.

XDATA. In FY13, the XDATA subproject began developing a framework for rapid composition of large data processing systems with advanced analytics and visualization for diverse missions and diverse platforms.

In FY14, the XDATA subproject worked on developing and demonstrating analytic tools for temporal and pattern analysis on a petabyte scale. In FY15, the subproject developed methods for interactive, iterative, and distributed analysis of diverse data at petabyte scale.

In FY16, the subproject was developing a scalable, robust framework for user-defined, adaptable visualizations. In FY17, this subproject is working to optimize software components and integrated applications to allow seamless integration into a user enterprise or mission environment.

Network Defense. In FY14, the Network Defense subproject developed analytics that detect structured network attacks within a single network. In FY15, the subproject created general-purpose algorithms for detecting novel classes of attacks across multiple networks.

In FY16, this subproject developed algorithms that use scanning events to provide indications and warning of coordinated adversary activities. In FY17, the subproject will optimize algorithms that detect anomalous behaviors and coordinated adversary activities through exercises using summary data and on-site evaluations.

Memex. In FY15, the Memex subproject developed domain-specific search engines to automatically discover, access, retrieve/extract, parse, process, analyze, and manage Web content in specified domains. In FY16, the subproject developed specialized search techniques for information discovery in networks of illicit activity. In FY17, this subproject will develop integrated applications from Memex components.

Distributed Battle Management. In FY14, the Distributed Battle Management subproject developed detailed requirements and initiated system engineering for a mission-focused team-level distributed battle management system intended to operate in a denied environment. In FY15, the subproject developed detailed system architecture for the distributed battle management system. In FY16, this subproject completed design of the overall DBM system, to include architecture, software components, concepts of operation, and integration strategy for expected host platforms.

In FY17, the subproject will demonstrate integrated DBM capabilities in live, virtual, and constructive simulations.

Quantitative Crisis Response. In FY15, the Quantitative Crisis Response subproject developed quantitative models to track the impact of Ebola on a population, with emphasis on social and economic factors. In FY16, the subproject refined quantitative models, content discovery, deep crawling, information extraction, and information relevance algorithms to support analysis and visualization of collected information. In FY17, this subproject will evaluate

Network Centric Enabling Technology

multiple end-to-end operational prototypes using automated, user, and team guided methods for Web content analysis and visualization.

Media Forensics (MediFor). In FY15, the Media Forensics subproject formulated approaches for automatically detecting when image and video files have been altered or manipulated. In FY16, the subproject developed advanced techniques for media fingerprinting. In FY17, this subproject will develop ways to detect manipulation in noisy, degraded and highly compressed media.

Science of Human and Computer Training. In FY17, this subproject will formulate human-machine

teaming strategies for military missions such as cyber defense and intelligence analysis.

Predicting Complex Operational Environments. In FY16, this subproject formulated computational models of political, military, economic, and social factors in complex operational environments to support military planning. In FY17, this subproject will work to introduce models that capture the impact of natural and human-mediated perturbations, such as water shortages, crop failures, and hoarding of critical resources, on theater security.

Funding

U.S. FUNDING

	FY15 QTY	FY15 AMT	FY16 QTY	FY16 AMT	FY17 QTY	FY17 AMT
RDT&E (U.S. DARPA)						
PE#0602702E						
Network Centric Enabling Technology	-	115.51	-	142.25	-	148.60
	FY18 QTY	FY18 AMT	FY19 QTY	FY19 AMT	FY20 QTY	FY20 AMT
PE#0602702E						
Network Centric Enabling Technology	-	170.53	-	174.58	-	210.61

All \$ are in millions.

Source: U.S. Defense Advanced Research Projects Agency (DARPA) FY17 RDT&E Budget Document

Contracts/Orders & Options

No contract information regarding the Network Centric Enabling Technology project has been made public. Consequently, no recent contracts have been identified.

Timetable

<u>Year</u>	<u>Major Development</u>
FY04	Automated Battle Management subproject begins applying and refining algorithms and software to assign autonomous combat vehicles to task-oriented teams
FY05	Combat Zones That See subproject starts developing, installing, and evaluating a Force Protection prototype
FY06	Home Field subproject demonstrates an effective man/machine interface to edit/update the extracted features
FY07	NEST subproject develops a prototype pulsing and sensing system to measure phenomenology, insertion losses, and radiation efficiency
FY08	Very High Speed Torpedo Defense subproject validates preliminary sensor and weapons concepts
FY09	EXACTO subproject develops a guidance system and maneuverable projectile
FY10	ICEWS subproject applies ICEWS data extraction and analysis methodologies in PACOM Terminal Fury exercise
FY11	Nexus 7 subproject develops techniques for simulation, visualization, inference, and prediction of social network dynamics
FY12	VIRAT subproject completes optimization of technologies to accommodate larger data sets

Network Centric Enabling Technology

<u>Year</u>	<u>Major Development</u>
FY13	Nexus 7 subproject develops techniques for processing timely, relevant information from traditional and non-traditional data streams
FY14	XDATA subproject develops and demonstrates analytic tools for temporal and pattern analysis on a petabyte scale
FY15	Network Defense subproject creates general-purpose algorithms for detecting novel classes of attacks across multiple networks
FY16	Memex subproject develops specialized search techniques for information discovery in networks of illicit activity
FY17	Distributed Battle Management subproject demonstrates integrated DBM capabilities in live, virtual, and constructive simulations

Worldwide Distribution/Inventories

Network Centric Enabling Technology is a project of the U.S. Defense Advanced Research Projects Agency.

Forecast Rationale

DARPA's Network Centric Enabling Technology project develops applications that integrate information arising from: 1) intelligence networks; 2) open and other external sources; 3) sensors and signal/image processors; and 4) collection platforms and weapon systems.

FI estimates that DARPA will spend more than \$1.9 billion on its Network Centric Enabling

Technology project over the next 10-plus years. This funding is being driven by the U.S. DoD's need to develop technology for use in network-centric operations.

Funding for the Network Centric Enabling Technology project will peak in FY22 and will average \$174 million per year from FY17 through FY20.

Ten-Year Outlook

ESTIMATED CALENDAR YEAR RDT&E FUNDING (in millions US\$)												
Designation or Program	High Confidence					Good Confidence			Speculative			Total
	Thru 2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	
MFR Varies												
NETWORK CENTRIC ENABLING TECHNOLOGY Military <> United States <> Department of Defense												
	912.87	146.50	168.00	172.00	208.00	210.00	218.00	209.00	212.00	216.00	215.00	1,974.50
Total	912.87	146.50	168.00	172.00	208.00	210.00	218.00	209.00	212.00	216.00	215.00	1,974.50