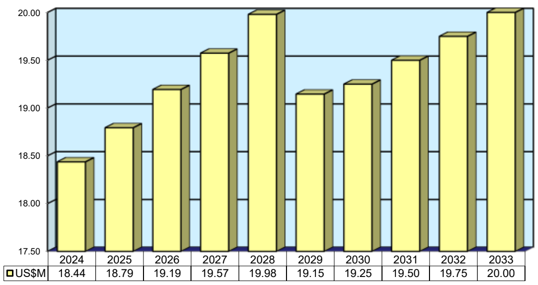
ARCHIVED REPORT

For data and forecasts on current programs please visit forecastinternational.com or call +1 203.426.0800

Cyber Applied Research

Outlook

- Cybersecurity is expected to remain one of the hottest defense electronics markets
- Self Securing Systems are a major focus for the program moving forward
- Funding for the development of cybersecurity methods and counter-technology expected to continuously increase through the forecast period and beyond



Funding Forecast
2024-2033

	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033
US$M	18.44	18.79	19.19	19.57	19.98	19.15	19.25	19.50	19.75	20.00

Orientation

Description. The U.S. Department of Defense's Cyber Applied Research project is part of the DoD Cyber Security Research program. It conducts research into both cybersecurity and computer network operations in order to harden key network and computer components, design new resilient cyber infrastructures, and increase the U.S. military's ability to fight against and survive cyberattacks. It also explores how to disrupt attack planning and execution at the nation-state level, and investigates and exploits new ideas in cyber warfare for agile cyber operations and mission assurance.

Sponsor

U.S. Department of Defense
The Pentagon
Washington, DC 20310

Status. Ongoing research and development.

Application. Provision of cybersecurity for U.S. DoD computer networks and systems. Cyber warfare.

Contractors

Prime

Raytheon	http://www.rtx.com/raytheon, 50 Apple Hill Dr, Tewksbury, MA 01876 United States, Tel: + 1 (978) 858-5000, Fax: + 1 (978) 858-9414, Email: ids@raytheon.com, RDT+E (RDT&E)

Contractors are invited to submit updated information to Editor, International Contractors, Forecast International, 75 Glen Road, Suite 302, Sandy Hook, CT 06482, USA; rich.pettibone@forecast1.com

Technical Data

The Cyber Applied Research project integrates computer network defense and computer network operations, addresses cyber operation problems, and fills capability and technology gaps as determined by assessments by the U.S. Office of the Assistant Secretary of Defense for Research & Engineering.

The effort develops technologies in the following areas:

Assuring Effective Missions. The Cyber Applied Research project develops the ability to assess and control the cyber situation in the mission context.

Behavioral Cyber Science. The point where hardware, software, and humans interact has become a jumping off point for a new area of research – behavioral cyber science. Cyber operations should be seen in the context of a larger socio-behavioral-technical domain.

Research in behavioral cyber science seeks to advance the understanding and technical rigor of modeling and predicting human responses to cyber activities and to discover ways to inject this understanding into the human aspects of cyber operations.

Future research must broaden the scope beyond the impacts of cyber actions on equipment and also include the impact of these actions on broader human behavior. Just as an adversary's behavior may be better understood using behavioral cyber science, behavioral science can be utilized to develop ways to improve the actions of cyber defenders and the performance of the cyber workforce. Data gleaned from observing the effects of various cyber operations on users' productivity, performance, and security will help the cyber workforce design better techniques and processes for use in cyber defense.

Self-Securing Systems. The pervasive nature of software-reliant systems in today's modern military creates new opportunities for sophisticated adversaries. The vast majority of DoD weapons systems, platforms, and networks rely on software to operate. Software can often be disrupted remotely, which necessitates a new kind of security to protect against cyberattacks.

Defending the software- and network-based aspects of critical weapon systems is challenging for a number of reasons, chief among them the advanced nature of the adversary in the cyber realm. The U.S. can expect future cyber adversaries to be well-funded, well-informed, and agile. Building weapon systems, platforms, and networks that can defend themselves in real time will be vital in protecting the U.S. against these adversaries.

The U.S. needs systems that can autonomously monitor and manage their own health and security posture through advanced sensing and perception, reasoning, and planning. Such systems could identify and classify threats much more quickly than a human operator, and, therefore, neutralize the threat more quickly and effectively.

However, researchers must be cognizant of the potential unintended consequences of turning security over to autonomous systems. Verification techniques must be developed to ensure that autonomous and dynamic system changes maintain correct mission-focused capabilities without introducing unintended vulnerabilities. Conversely, developing techniques to track and audit actions taken by autonomous systems is crucial to ensuring that direct control can be reasserted, potentially reversing some actions if necessary.

Precise Cyber Effects. When compared to traditional methods of kinetic warfare, cyber conflict is still relatively new and untested. Cyber operators often have incomplete information about their target prior to completing an action. The lack of a complete picture makes it difficult to predict the precise outcomes or collateral damage caused by a cyber operation. In this type of uncertain environment, military leaders may be acting with an undue sense of caution in using cyber capabilities. Improved technology and techniques for quantifying cyber effects, estimating their cost and effectiveness, predicting consequences, and ensuring precise effects will help both to limit collateral damage and to ensure that a chosen action has the intended effect on the adversary. Highly precise and predictable cyber effects can also achieve mission goals despite the presence of both incomplete and maliciously created false information.

Applied Mathematics. Mathematics is intrinsically linked to all branches of science and technology. Cybersecurity research is no exception. Broadly, there is a need for an array of modeling techniques, both informal and formal, backed by various rigorous mathematical theories, to capture and support the richness of the cyber domain. This area of research is needed to help characterize the cyber domain and cybersecurity, maintain the integrity of data, harden systems, and analyze potential solutions. Continued research in mathematical theory beyond the basic research level is crucial to maintaining and increasing the security of cyber systems.

The U.S. Cyber Command is responsible for overall DoD cybersecurity in areas of offensive and defensive countermeasures as well as R&D.

Source: U.S. DoD

Program Review

A discussion of the specifics of each of the program's technical areas of focus, and recent activity, follows.

Assuring Effective Missions. In FY13, the Cyber Applied Research project developed techniques for course-of-action development and analysis. In FY14, it worked on identifying critical assets and potential rogue workflows. The project assessed the effectiveness of agility mechanisms and moving target techniques against "advanced persistent threats" during FY15. In FY16, efforts focused on development of a cloud-based defense architecture system. The prototype was tested in FY17.

Work concluded in FY18 with proof-of-concept testing of a machine finger-printing algorithm. In addition, research papers on deep learning, natural language processing, entity extraction/characterization, and workflow discovery were produced.

Behavioral Cyber Science. The Behavioral Cyber Science effort identifies and validates hypotheses. The research identifies sensor data that correlates strongly with human responses. In FY18, this program began a research effort aimed at addressing scientific challenges in order to broaden the scope of cyber activities through an understanding of human behavioral sciences. Work continued through FY19 and into FY21 with development of a workflow monitoring prototype.

Plans for FY21 also included demonstrating a prototype of the Contextualized Operator Perspective work support system, measuring increases in Cyber Protection Team efficiency via field exercises.

FY22 plans included advancing the understanding and technical rigor of modeling and predicting human responses to cyber activities that enhance cyber operations through planning and training. They also included exploring the interaction between computers and human behavior, moving beyond electronic signals (ones and zeroes) to enable development of new insights into human behavior.

Self-Securing Systems. Begun in FY18, this effort focuses on developing novel adaptive techniques for modeling adversary options and predicting the security of future system configurations, even under "unknown attacks." It also started research and development of cyber immunology so that systems can "monitor [cyber] health and develop identification/classification mechanisms for cyber threats."

In FY20, efforts were centered on the continued development of "Self-Securing Systems: Autonomous Cyber Defense." The project uses deception techniques based on human operator defender goals.

FY21 efforts can be broken down into three categories:

- Demonstrate and quantify a cyber-resilient command and control software-defined network architecture in the U.S. Army's C2/Internet of Battle-Things environment.
- Develop a group vehicle threat and mitigation scenario to highlight existing countermeasures to supply chain threats as part of an overall cyber resilience demonstration.
- Consolidate data from DoD Cybersecurity S&T investment areas that address gaps and accelerate the adaptation of promising results into military vehicle platforms and commercial vehicles.

FY22 plans called for integrating formal methods into a high security and high agility DevSecOps (development, security, operations) development process. Plans also called for expanding existing cyber research in order to, according to the DoD, "add ensembles helping to reduce uncertainty surrounding predicted effect types and their measured magnitudes within critical infrastructures."

Cyber Applied Research Archived MAR

Precise Cyber Effects. In FY17, progress was made toward improving the accuracy and precision of cyber effects in order to achieve cyber mission impacts comparable to precision bombing campaigns. This work was followed up in FY18 with the development of modeling techniques, based on limited data, capable of predicting the range of possibilities that might result from a planned cyber effect. This work continued into FY21.

Other efforts focused on the U.S.-Australian bilateral Mission Assurance Research Collaboration (MARC) project that analyzes data collected during the Talisman Sabre 2017 command post exercise by applying mission mapping algorithms and machine learning processes.

FY20 activity was focused on addressing 5G security issues and spectrum opportunities to augment Future Autonomous Battlespace Radio Frequency with integrated communications. This research will lead to the exploration of 6G standards.

FY21 plans called for demonstrating cyber-physical system dependency using modeling- and simulation-based discovery and integrating an improved discovery process into the evolving Cyber Joint Munitions Effectiveness Manual within the operations community.

FY22 plans called for expanding existing cyber research in order to, according to the DoD, "add ensembles that will help reduce uncertainty surrounding predicted effect types and their measured magnitudes within critical infrastructures." They also called for the examination of statistics-based methods to develop more robust causality models of system performance and failure.

Applied Mathematics. The Mathematical Foundations of Cybersecurity portion of the project funds research into the development and enhancement of foundational work underpinning cyber technology in the area of advanced mathematics. From FY18-FY20, research was conducted into mathematical logic and formal methods, network science, information theory, decision sciences, risk analysis, and modeling and simulation.

FY21 plans were to explore the use of AI as a force multiplier to enhance human-machine teaming for robust decision-making, develop AI-augmented capabilities across the cyber kill chain, build autonomous cyber defense capabilities, and develop AI-enabled technologies for cyber application.

FY22 plans called for exploring the technical rigors and "science-based, repeatable, automated, and affordable methods for quantitatively measuring cyber resilience offered to military engineered artifacts."

Funding

U.S. FUNDING

	FY22 QTY	FY23 QTY	FY24 QTY	FY25 QTY	FY26 QTY	FY27 QTY	FY28 QTY	FY29 QTY
RDT&E (U.S. OSD)								
PE#0602668D8Z: Cyber Security Research								
Project 003: Cyber Applied Research	24.59	42.14	17.44	17.79	18.19	18.57	18.98	N/A

All $ are in millions.

N/A = Not Available

Source: U.S. Department of Defense FY24 RDT&E budget document

Contracts/Orders & Options

No contract information regarding the Cyber Applied Research project has been made public.

Worldwide Distribution/Inventories

Cyber Applied Research is a project of the **U.S. Department of Defense**.

Forecast Rationale

In order for U.S. military forces to conduct effective operations, there is a requirement for resilient and reliable networks, information, and weapons systems in a world of ever-evolving technological advancement. Both the number and sophistication of threats in cyberspace are rapidly growing, making the improvement of cybersecurity critical for all Department of Defense systems seeking to counter those threats and assure the department's missions.

The Cyber Applied Research project meets this need for improved cybersecurity. This project is part of the larger U.S. DoD Cyber Security program. This program focuses on innovative and sustained research in both cybersecurity and computer network operations. It is tasked with the development of new concepts to harden key network and computer components in addition to designing new and resilient cyber infrastructures. The program also increases the military's ability to disrupt, fight, and survive cyberattacks.

The future of the project sees the development of a means to measure the state of health in cybersecurity and explore and exploit new ideas in cyber warfare for agile cyber operations and mission assurance. It will also explore how to protect tactical networks, weapons systems, and platforms. This effort is unique in that it integrates both the defensive and offensive cyber research from each of the services to develop interoperable, defense-wide technology options targeted to meet combatant command-level requirements. More specifically, by increasing cross-laboratory collaboration, this program is able to take service-specific technologies and expand their applications to the joint forces.

The growing reliance on data transmission and networking has been accompanied by an increase in cyber system hacking. As a result, cybersecurity is one of the hottest defense electronics markets. Funding for the development of cybersecurity methods and counter-technology is expected to increase through the forecast period and beyond.

It should be noted that since 2018, the project has focused on the development of self-securing systems, a means of defense that accounts for human error. This sort of technology will be critical for future security.

Ten-Year Outlook

ESTIMATED CALENDAR YEAR RDT&E FUNDING (in millions US$)												
Designation or Program		**High Confidence**				**Good Confidence**			**Speculative**			
	Thru 2023	**2024**	**2025**	**2026**	**2027**	**2028**	**2029**	**2030**	**2031**	**2032**	**2033**	**Total**
MFR Varies												
Cyber Applied Research <> United States <> Department of Defense												
	224.22	18.44	18.79	19.19	19.57	19.98	19.15	19.25	19.50	19.75	20.00	193.63
Total	224.22	18.44	18.79	19.19	19.57	19.98	19.15	19.25	19.50	19.75	20.00	193.63