Statement by Arati Prabhakar

Director, Defense Advanced Research Projects Agency (DARPA)

Before the

Subcommittee on Emerging Threats and Capabilities

Armed Services Committee, U.S. Senate

Strategy and Implementation of the Department of Defense's Technology Offsets Initiative in Review of the Defense Authorization Request for Fiscal Year 2017 and the Future Years Defense Program

April 12, 2016

NOT FOR PUBLICATION UNTIL RELEASED BY THE SUBCOMMITTEE

Chairman Fischer, Ranking Member Nelson and Members of the Subcommittee, thank you for the opportunity to testify before you today. I am Arati Prabhakar, Director of the Defense Advanced Research Projects Agency, better known as DARPA. It is a pleasure to be here with my colleagues from the Department of Defense (DoD) research and development community to discuss DARPA's investments in breakthrough technologies for national security and in particular our contributions to the Department's Third Offset Strategy.

For nearly six decades, DARPA has played a particular role in this community of government innovators, and in the larger U.S. technology ecosystem: to pursue extremely challenging but potentially paradigm-shifting technologies in support of national security. Today I will focus my remarks on DARPA's role in the development of technologies to offset the advanced threats that our military and our Nation will face in the years ahead, and on the next generation of advanced military capabilities to deter and if necessary defeat highly sophisticated adversaries.

A CHANGING WORLD

Our senior military and civilian leaders face a world of kaleidoscopic uncertainty today and into any foreseeable future. The daily fare includes a noxious stew of violent extremism, terrorism, and cross-border criminal activity. At the same time, the actions and intentions of nation states in every region are increasingly demanding DoD's focus and attention. Arsenals in some of these nations have grown substantially in the past decade, and recent provocative actions by nations around the world have made clear that their capabilities have grown as well. Moreover, several U.S. peer adversaries today boast first-rate scientists, engineers, laboratories and industries, raising the stakes for future capabilities considerably. Our challenge at DARPA and for DoD is to maintain a significant advantage for military and national security purposes against this competitive and shifting backdrop.

To achieve this advantage, the Department has embarked on an important shift in recent years to reenergize its ability to invent, experiment with and operationalize advanced military capabilities that will be critical to deter and if necessary defeat the emerging great powers of this century. DoD's Third Offset Strategy and its Long Range Research and Development Plan (LRRDP) embody this important shift.

Technological capabilities are only one dimension in these strategies. This is where DARPA makes it contribution. Because DARPA's core mission is to make pivotal early investments in breakthrough technologies for national security, the Agency is always looking beyond the challenges of the moment to anticipate and create options for the future. As a consequence, DARPA plays two roles in the Department's Third Offset Strategy and the LLRDP. The first role is the obvious one: developing and demonstrating critical core technologies for these new strategies through the execution of a wide portfolio of DARPA programs. A second role that DARPA plays is sharing its expertise and perspectives on future technologies to inform how these Departmental strategies are shaped.

These two roles are reflected in twin principles that guide our thinking at DARPA. One principle is that in the years ahead, the most powerful defense systems will come from the tight integration of leading-edge commercial technologies and highly specialized military technologies. You will see this approach in many of our programs, from tablets with added encryption for close air support to state-of-the-art digital electronics with added DoD-unique radio chips for leapfrog radio frequency (RF) systems. The second key principle is that future U.S. military success will lie in building systems that are designed to evolve, grow and adapt.

This second principle is critical in light of a significant difference between the Third Offset and previous offsets. While previous offsets had as their goal bursts of accelerated technological progress to provide comfortable, multi-decadal leads over our adversaries, it is unlikely the United States will again enjoy such monopolies on advanced technologies. Unlike the decades following the Second World War, global connectedness and the democratization of sophisticated scientific and engineering skills and capabilities make the maintenance of such steep technological gradients all but impossible today. That means that rather than striving for a temporary, static advantage for a period of years, the Third Offset must deliver immediate advantages with built-in evolutionary capacities *and* a portfolio of more fundamental, enabling technologies that can support a long-term succession of iterative advances and assurance of ongoing momentum and pace. In short, we must design not just a new point of capability, but new curves of expanding capability over time.

In similar fashion, my testimony today will focus on two collections of DARPA research programs relevant to the Department's Third Offset Strategy. The first collection includes examples of efforts that are focused on the development of

next-generation technologies to counter next-generation adversaries. The second collection includes examples of efforts that are more fundamental in nature and are laying the foundation for advances even further in the future. Within each of these two categories, I have organized our efforts into three groups, representing three degrees of technological maturity: technologies already being piloted or used ("Adoption and Impact"), those currently in development ("Technical Progress") and those that are inspiring new investments but that have hallmarks of longer-term, outsized potential ("New Opportunities").

DARPA'S INVESTMENT PORTFOLIO

Next-generation Technologies to Counter Next-generation Adversaries

DARPA aggressively pursues technologies with the potential to expand DoD's range of tactical and strategic options and impose technological surprise on our adversaries. Our work spans every traditional domain of conflict, including maritime, ground, air and space, as well as the cyber and biological domains. And it embraces not only traditional military hardware but also core mission systems such as communications, radar, electronic warfare, and position, navigation and timing systems. At DARPA, a crosscutting theme across all of these areas is the need to escape from reliance on today's highly capable but monolithic and expensive platforms in favor of a more diversified array of platform architectures that are smaller and heterogeneous and thus harder to target, less expensive and more easily upgraded, and can ultimately produce more powerful effects than any single platform by itself. DARPA's challenge is to imagine, design and develop the separate but networked components of this new paradigm and demonstrate the power of complex but seamless systems of systems.

Adoption and Impact

Communications Under Extreme RF Spectrum Conditions (CommEx)
DARPA's CommEx program is developing technologies that can characterize the jamming environment and then actively suppress enemy jamming, so aircraft can still communicate with each other in a highly contested RF environment. Initial components of CommEx technology are part of a planned upgrade to the widely used Link 16 air-to-air data network.

Cognitive Electronic Warfare (EW)

DARPA's Advanced RF Countermeasures (ARC) and Behavioral Learning for Adaptive Electronic Warfare (BLADE) programs are investing in the technologies needed to rapidly react to dynamic electromagnetic spectrum signals from adversary radar and communications systems. These programs are applying machine learning—computer algorithms that can learn from and make predictions from data—to react in real time and jam signals, including new signals that have not yet been cataloged. DARPA is working with the Services to transition technologies derived from the field of cognitive electronic warfare into the F-18, F-35, Army Multi-Function EW program, and Next Generation Jammer.

Power Efficiency Revolution for Embedded Computing Technologies (PERFECT)

DARPA's PERFECT program is developing revolutionary approaches to improving the energy efficiency of DoD computational systems, an improvement that will embed significantly increased computing capabilities including modern learning algorithms on power-limited platforms such as UAVs. Resulting technologies are transitioning to both commercial and government users, with the National Reconnaissance Office adopting them for new, radiation-hardened circuit architectures that enable extremely high data-throughput next-generation space systems. A consortium of companies including Google, HP and Oracle, is pursuing power-efficient open-source hardware, such as RISC-V open-source cores developed in part with PERFECT funding.

Long Range Anti-Ship Missile (LRASM)

DARPA and the Office of Naval Research (ONR) collaborated to develop the Long Range Anti-Ship Missile (LRASM), an advanced anti-ship missile capable of operating at extended ranges with reduced dependency on intelligence, surveillance and reconnaissance (ISR). The collaboration began as a technology demonstration effort in early 2009. The first two flight tests were conducted in the fall of 2013, during which all demonstration objectives were met. To ensure speedy and seamless development and deployment of this new capability, DARPA created and at first led a LRASM Deployment Office (LDO) with the Navy and Air Force, as LRASM transitioned to a Navy Program of Record. A third flight test, conducted in February 2015, further assessed technical maturity. This past December the Navy took over the LDO directorship, marking the successful transition of a model collaborative effort to address a pressing strategic need.

Research on Fresh Approaches for Computer Security

DARPA's Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) program was a basic research effort that designed new computer systems that are highly resistant to cyber attack. The technology development has recently concluded, and CRASH-developed software is now being incorporated in the commercial and military arenas. One university performer started a company based on CRASH research; this led to an announcement from HP in September 2015 that its new line of printers would feature this software to enhance their security. DARPA is coordinating transitions to the Navy and the Defense Information Systems Agency (DISA). For example, the aforementioned software is now being transitioned to the Naval Surface Warfare Center to protect shipboard control systems from cyber attack, and other CRASH software is being transitioned to offer similar protection for DoD command and control servers. Additionally, the Department of Homeland Security and the Air Force Research Laboratory have been working together to test and evaluate CRASH technology in multiple devices. Because the cyber-attack surface is vast and diverse, each of these transitions makes a contribution to the Nation's cybersecurity by taking a class of threats off the table.

Active Authentication

Passwords are cumbersome and imperfect authentication systems for use on information systems, and most systems have no way of verifying that the user who was originally authenticated is the user still in control of the keyboard. DARPA's Active Authentication program is addressing this problem by developing novel ways of validating identity—ways that focus on unique aspects of the individual through the use of software-based biometrics, including behavioral traits such as subtleties in keystroke style or screen-swipe patterns. Although these biometrics may never completely replace passwords, they can provide an added layer of assurance of a user's identity—and DARPA-developed systems have begun to make their way into commercial products, where they are already in use by millions of users. One version, for example, has been incorporated into Google's new Android behavioral authentication system announced last June; others are being piloted by several banks in the United States and Europe, where they have helped secure more than 1.5 million transactions; and yet others are being explored by the National Institute of Standards and Technology for possible use within the National Strategy for Trusted Identities in Cyberspace (NSTIC).

Technical Progress

Unmanned Surface Vessel for Long-Duration Missions

The Anti-Submarine Warfare (ASW) Continuous Trail Unmanned Vessel (ACTUV) program has designed, developed and constructed an entirely new class of ocean-going vessel—one able to traverse the open seas for months and over thousands of kilometers without a single crew member aboard. The 130-foot ship is designed to robustly track quiet diesel electric submarines. But of broader technical significance, it embodies breakthroughs in autonomous navigational capabilities with the potential to change the nature of U.S. maritime operations. Specifically, ACTUV is endowed with advanced software and hardware that enables full compliance with maritime laws and conventions for safe navigation—including international regulations for preventing collisions at sea, or COLREGS—while operating at a fraction of the cost of manned vessels that are today deployed for similar missions. ACTUV was recently transferred to water at its construction site in Portland, Ore. It is scheduled to be christened on April 7, with open-water testing to begin this summer off the California coast.

XS-1

The objective of the Experimental Spaceplane XS-1 program is to demonstrate the technology needed to fabricate and fly a reusable aircraft to the edge of space—and be able to do so 10 times in 10 days, to demonstrate "aircraft-like" operability, cost efficiency and reliability. Success would radically alter the current space-access equation in which launches must be arranged years in advance. That bottleneck not only adds to the cost of placing national security payloads on orbit but also forces an increase in the complexity of the payloads themselves. In an era of declining budgets and proliferating foreign threats to U.S. air and space assets, routine, affordable and responsive access to space is essential to enabling new military space capabilities and rapid reconstitution of space systems during crisis. Specific goals of XS-1 include an ability to deploy a small expendable upper stage to launch a 3,000-pound spacecraft to low-Earth orbit at a cost of $5M, ten times less than today's launch systems.

System of Systems for Air Superiority

In recent years, DARPA has started a collection of programs that aims to develop and demonstrate technologies that together can dramatically advance air combat capabilities against sophisticated adversaries by coordinated deployment of distributed assets with diverse capabilities rather than reliance on densely consolidated capabilities on large, expensive and unwieldy platforms. Key to these

efforts is the approach of integrating new capabilities with existing systems to achieve cost leverage against near-peer adversaries and to continuously progress faster and at lower cost than traditional monolithic platform-based approaches.

DARPA's System of Systems (SoS) Integration Technology and Experimentation (SoSITE) program is developing novel architectures—combinations of different types of aircraft, weapons, sensors and mission systems—that distribute air warfare capabilities across a large number of interoperable manned and unmanned platforms. In the last year, we developed an analytical capability to compare the mission performance and cost leverage of alternative architectures and found several promising approaches to achieving air dominance in highly contested environments. The technical and operational risks associated with these approaches are being analyzed this year to provide the basis for our flight experimentation program in the next phase of the program.

The Distributed Battle Management (DBM) program is one key component of the Agency's system-of-systems vision. Current battle management systems offer only limited automated aids to help warfighters comprehend and adapt to dynamic situations. Adding more elements to the SoS architecture—more unmanned aircraft, missiles and mission systems—will exacerbate the battle management challenge, as will the degraded communications of a highly contested environment. The DBM program seeks to develop appropriately automated decision aids to assist airborne battle managers and pilots manage air-to-air and air-to-ground combat. In the initial phase of the program, we developed algorithms to disseminate hostile track data using limited communications across tactical data links. These algorithms achieved high accuracy while requiring less communications capacity then standard approaches. We also developed algorithms for automatic control of UAVs in conducting air-to-air and air-to-surface engagements. In the next phase of the program, these algorithms will be integrated with appropriate human-computer interfaces. The resulting capability will be evaluated by pilots and operators in a virtual simulation environment.

<u>High-Assurance Cyber Military Systems (HACMS)</u>

Embedded processors are the ubiquitous computational brains in DoD systems, but along with their valuable capabilities comes an ever-growing attack surface for cyber malfeasance. DARPA's HACMS program is developing tools and methods for the design and construction of high-assurance cyber-physical systems—scaling the mathematics of formal methods to create devices effectively "unhackable" for specified properties. DARPA has applied these techniques initially to a Little Bird

helicopter, using a HACMS microkernel to give the mission computer a cyber retrofit. In a flight test, a red team was unable to attack the helicopter's controls, despite the fact that the team was given access to the platform and its software, including its source code.

Cyber Grand Challenge (CGC)

It typically takes months or years for a software bug to be identified and patched—a period of time increasingly being taken advantage of by digital miscreants, and a vulnerability window not likely to shrink as long as the process for identifying and repairing such flaws remains mostly manual and artisanal as it is today. CGC is a DARPA-sponsored competition that aims to accelerate the development of automatic defensive systems capable of reasoning about flaws, formulating patches and deploying them on a network in real time. By acting at machine speed and scale, these technologies may someday overturn today's attacker-dominated status quo. Seven teams from across the United States qualified last year to compete in the CGC final event, which will take place August 4, 2016, live on stage, co-located with the DEF CON 24 conference in Las Vegas.

Mining and Understanding Software Enclaves (MUSE)

DARPA's MUSE program seeks a radical rethinking of the way we conceive and maintain software, by integrating foundational ideas from formal methods and machine learning to an ever-growing corpus of open-source software. The techniques being developed under MUSE are intended to discover deep semantic properties from the programs found in its corpus. These properties drive two distinct analytic tasks. The first enables automatic identification and repair of software bugs by recognizing anomalous structure based on properties found in similar previously analyzed programs; the second synthesizes new software behavior from existing corpus elements based on formal specifications. To date, DARPA has assembled a software corpus of more than 20 terabytes and has successfully applied its technologies to automatically synthesize a provably correct implementation of sophisticated cryptographic protocols such as Advanced Encryption Standard (AES), and repair well-known security vulnerabilities such as Heartbleed.

New Opportunities

Maritime System of Systems

DARPA has made important technical progress towards future air dominance through the development of a systems-of-systems approach. Now, through its

Cross Domain Maritime Surveillance and Targeting (CDMaST) program, DARPA is extending this model into the maritime domain. The program will be developing technologies to disaggregate various functions across multiple lower cost, upgradable and in many cases unmanned platforms on the sea surface and underwater. By distributing the functions of position, navigation and timing; communications; command and control; and networking and logistics across large expanses, this architecture will force the adversary to defend a very wide area at high cost, inverting the cost curve for securing the maritime environment.

Leading-edge Electronics with Built-in Trust

Under the hood of every military system are the electronic components that are its brains, eyes and ears, but DoD has struggled for decades with contradictory demands in designing, sourcing and maintaining these vital components. Military systems need the most capable integrated circuit (IC) technology to do their phenomenally difficult computational or signal-processing tasks with the limited power available on a missile or aircraft. Yet designing custom ICs continues to grow more complex, and fewer teams are able to commit the time and money for custom design, even in the commercial world. At the same time, security is essential for military applications but semiconductor production has globalized, with diminishing U.S.-owned, U.S.-sited production capacity at the leading edge of technology, and supply chains now crossing multiple national borders. And while IC technology progresses at a pace set by the commercial sector, DoD needs access to components for decades. To address this group of challenges, DARPA is building a cluster of programs aimed at creating new options for DoD.

DARPA's Trusted Integrated Circuits (TRUST) program is developing technologies that will ensure the trustworthiness of ICs used in military systems, even when those components have been designed and fabricated under untrusted conditions. TRUST makes a radical departure from conventional verification approaches, using advanced metrics to identify with increasing efficiency ICs that have been maliciously attacked while reducing the incidence of declaring good circuits to be bad.

The Supply Chain Hardware Integrity of Electronics Defense (SHIELD) program aims to eliminate counterfeit ICs from the electronics supply chain by inserting into the packaging of these components minuscule "dielets"—chips tinier than a grain of salt, with embedded encryption, sensors, near-field power and communications capabilities—to detect any attempt to tamper with the relevant electronics. Dielets are being designed to incorporate passive, unpowered sensors

capable of capturing attempts to image, de-solder, de-lid or image the IC; mechanical processes that make the dielet fragile and prevent intact removal from its package; and a full encryption engine and advanced near-field technology to power the dielet and provide communications, to make counterfeiting too complex and time-consuming to be cost effective.

DARPA's Integrity and Reliability of Integrated Circuits (IRIS) program is developing techniques to provide system developers the ability to derive the function of digital, analog and mixed-signal ICs non-destructively, given limited operational specifications. These techniques include advanced imaging and device recognition of deep-sub-micron circuits, as well as computational methods to determine device connectivity. The program is also working to better understand circuit aging systems and to produce innovative methods of device modeling and analytic processes to determine the reliability of integrated circuits by testing a limited number of samples. Resulting technologies will help ensure that DoD microelectronics reliably perform as expected and only as expected by revealing potential compromises due to manufacturing defects, counterfeiting or the addition of malicious components.

The Circuit Realization at Faster Timescales (CRAFT) program seeks to develop new fast-track circuit-design methods, multiple sources for IC fabrication and a technology repository that will facilitate reuse of proven solutions. To achieve its goals, CRAFT seeks to shorten the design cycle for custom integrated circuits by a factor of 10 (on the order of months rather than years); devise design frameworks that can be readily recast when next-generation fabrication plants come on line; and create a repository so that methods, documentation and intellectual property need not be reinvented with each design and fabrication cycle.

Cybersecurity for the Grid

Embraced by two vast oceans and sharing borders with only two nations—both of them allies—the United States has long enjoyed a degree of insular security. But our critical infrastructure's growing dependence upon cyber systems inherently accessible even from long distances means that the prospect of attacks against the homeland must now be taken very seriously. Indeed, with cost pressures having driven the integration of conventional information technologies into the nation's dispersed industrial control systems, today'sgrid is increasingly vulnerable to cyber attack, either through direct connection to the Internet or via interfaces to utility information technology systems. DARPA's recently launched Rapid Attack Detection, Isolation and Characterization Systems (RADICS) was created to

develop automated systems that would help cyber and utilities engineers restore power within seven days of an attack that overwhelms the recovery capabilities of power providers. RADICS's goals include the development of advanced anomaly-detection systems with high sensitivity and low false-positive rates, based on analyses of the power grid's dynamics; the development of systems that can localize and characterize malicious software that has gained access to critical utility systems; and the design of a secure emergency network that could connect power suppliers in the critical period after an attack.

Foundational Technologies to Support Long-term, Successive Advances

In addition to pursuing the kinds of game-changing technologies described above, DARPA has the responsibility for investigating research areas that are so new and unformed as to exist more as inklings than disciplines. This is the part of our portfolio that anticipates and prepares for varieties of threats that are still poorly understood but have the potential to wreak entirely new kinds of havoc—including the fast-evolving field of biology, which has outsized potential for strategic surprise but has not traditionally been at the core of the Nation's national security framework. It is in this part of DARPA's portfolio that the seeds of future offsets are being discovered and cultivated. And while the outcomes of these efforts are inherently less predictable than those of other programs, these efforts also have the most dramatic long-term potential to generate truly revolutionary capabilities that can counter categories of risk hardly imaginable today.

Adoption and Impact

Additive Manufacturing for Performance Applications

Despite its revolutionary promise, additive manufacturing is still in its infancy when it comes to understanding the impact of subtle differences in manufacturing methods on the properties and capabilities of resulting materials. Those uncertainties have slowed the reliable mass production of additively manufactured structures with demanding specification requirements, such as structural components for aircraft and other military systems. To overcome this problem, DARPA's Open Manufacturing (OM) program is building and demonstrating rapid qualification technologies that comprehensively capture, analyze and control variability in the manufacturing process to predict the properties of resulting products. Success could help unleash the potential time- and cost-saving benefits of advanced manufacturing methods for a broad range of defense and national security needs.

DARPA's OM framework and data schema are already being used by the Navy in their efforts to produce flight-critical metallic components with an additive-manufacturing-certified Technical Data Package, with plans to field a set of flight-critical metallic components for the V-22, H-1, and CH-53K platforms by 2017. Manufacturing pedigree considerations, such as a baseline set of standards and schema for additive manufacturing data collection, are being provided by the OM Manufacturing Demonstration facilities at Penn State and the Army Research Laboratory. In another application, advanced manufacturing approaches for bonded composites could enable aircraft wings and fuselages, for example, to be built and joined together without the thousands of rivets and fasteners currently required, significantly reducing manufacturing costs and time and lowering operating costs by making aircraft lighter.

Accurate, Specific Disease Diagnostics on the Spot

The challenge of tracking the spread of infectious disease is exacerbated by the fact that the only way to know precisely which pathogen ails a patient is to draw blood, send it to a lab, and often wait days to hear the result. The Mobile Analysis Platform (MAP) point-of-care diagnostic device is a simple, rugged, handheld, battery-operated instrument that rapidly identifies a range of infectious diseases. Developed under DARPA's Prophecy program, it enables low-cost and robust molecular diagnostics within 30-45 minutes in areas where neither a laboratory nor a secure cold chain is available. And because the device provides instant wireless transmission of test results and location data, it can provide invaluable real-time epidemiological data during outbreaks of fast-moving diseases such as Ebola. DARPA is already engaged in clinical testing of the device with the Naval Health Research Center and the U.S. Military HIV Research Program, and will conduct testing with the Marine Corps Warfighting Laboratory this year during military exercises in the United States and West Africa. In addition, DARPA recently initiated development of a MAP assay for Zika virus.

Biologists, Start Your Startups!

For many of the technologies driven by DARPA's Biological Technologies Office, the path to impact runs through commercialization. Several recent examples point to early progress in this regard.

DARPA's Autonomous Diagnostics to Enable Prevention and Therapeutics (ADEPT) program is creating a new technology base to outpace the spread of natural or engineered diseases and toxins through the development of rapid

diagnostics, novel vaccines, new methods for drug delivery and entirely new approaches to providing populations with antibody-derived immunity. Among other technology and business successes resulting from ADEPT are a DARPA-enabled spin-off that has since received more than $25 million in venture funding for further development of a novel diagnostic platform and another small biotech company for which DARPA provided the initial research funding that went on to receive venture funding to continue development of tissue-integrated biocompatible sensors.

DARPA's Microphysiological Systems (MPS) program—better known as the Agency's foray into "organs-on-a-chip" technology—is developing a platform that uses engineered human tissue to mimic human physiological systems as a means of testing the safety and effectiveness of candidate drugs, vaccines or other biomedical countermeasures. In one of many applications, two DARPA performers are collaborating to understand the liver toxicity that can be caused by biological therapeutics—a common reason why otherwise promising drug candidates fail in clinical trials. Among the program's business successes are a start-up microfluidics company spun off from the research that DARPA had funded, which has since gone on to raise more than $10 million in venture funding.

Technical progress

Harnessing Extreme Physics

Through a number of ambitious basic science programs, DARPA is pushing the limits of the physical sciences, opening new possibilities for ultra-precise measurements and unprecedented control over fundamental phenomena. Among them:

The science of quantum communications—in which single photons from entangled photon pairs are transmitted over a distance—offers the possibility of unconditionally secure communication because the act of measuring a quantum object necessarily changes it. For quantum communications to be practical, however, several technological barriers must be overcome. DARPA created the Quiness program to investigate novel technologies capable of high-rate, long-distance quantum communications. Recent demonstrations through Quiness of technologies to capture, manipulate and re-transmit photons without in effect measuring them are truly significant. This is because theorists in Quiness were able to prove from fundamental quantum principles that such "quantum repeater"

technologies are the only way to achieve quantum communications over trans-continental distances.

Many defense-critical applications—the Global Positioning System (GPS) and the Internet, for example—demand exceptionally precise time and frequency standards. Today's systems, however, rely on 1950s atomic physics technologies. Recent advances in optical atomic systems give promise to a new generation of optical atomic clocks and quantum metrology that stands to transform numerous DoD applications. The Quantum-Assisted Sensing and Readout (QuASAR) program is developing new quantum control and readout techniques to provide a suite of measurement tools that will be broadly applicable across disciplines, with likely applications relating to biological imaging, inertial navigation and robust global positioning systems. Recently the program demonstrated the world's most accurate clock with a total uncertainty of 2 parts in 10^{18}, or about 10,000 times better than GPS clocks. This means that if the clock began ticking at the Big Bang nearly 14 billion years ago it would be accurate to better than one second today. Clocks of this caliber could lead to improved positioning and navigation, and enable novel imaging and geological sensing techniques.

DARPA's Ultrafast Laser Science and Engineering (PULSE) program is developing the technological means for engineering improved spectral sources, such as ultra-fast optical lasers—advances that in turn could facilitate more efficient and agile use of the entire electromagnetic spectrum and generate improvements in existing capabilities such as geolocation, navigation, communication, coherent imaging and radar, and perhaps give rise to entirely new spectrum-dependent capabilities. Recent PULSE demonstrations include synchronization of clocks with femtosecond precision across kilometers of turbulent atmosphere, corresponding to a 1,000-fold improvement over what is possible using conventional radio-frequency techniques.

New opportunities

Changing the Security-Privacy Trade-off

DARPA's Brandeis program will explore technologies that could help break the tension between maintaining privacy and being able to tap into the huge value of data. Rather than having to trade off between these important goals, Brandeis aims to build a third option, enabling safe and predictable sharing of data while reliably preserving privacy. Assured data privacy could help open the doors to a number of security-relevant goals, from collections of publicly available data that can help

predict military movements or emergency situations to early evidence of cyber attacks on shared networks—applications that in some environments could be difficult to fully implement without assurances of privacy.

Communicating with Computers

A new and powerful wave of artificial intelligence (AI) is sweeping commercial and military applications today. Based on recent major advances in machine learning—research that was sponsored in part by DARPA—this generation of AI is fueling fields as disparate as search, self-driving cars and financial trading in the commercial world and battle management, electronic warfare, cybersecurity and information operations in the national security realm. I have touched on some of these examples in my testimony today.

Despite this significant technical progress, however, the ways in which we humans interact with machine systems are still quite limited compared to human-to-human interactions. DARPA's Communicating with Computers (CwC) program is a basic research effort to explore how to facilitate faster, more seamless and intuitive communication between people and computers—including how computers endowed with visual or other sensory systems might learn to take better advantage of the myriad ways in which humans use contextual knowledge (gestures and facial expressions or other syntactical clues, for example) to enrich communication. Ultimately, advances from this program could allow warfighters, analysts, logistics personnel and others in the national security community to take fuller advantage of the enormous opportunities for human-machine collaboration that are emerging today.

All the Light We Cannot See

Light that enters the eye or the lens of a camera carries much more information than is typically retrieved by viewers, including numerous details about where it has been and what it has experienced. DARPA's Revolutionary Enhancement of Visibility by Exploiting Active Light-fields (REVEAL) program seeks to unlock information in photons that current imaging systems discard. The program is first developing a comprehensive theoretical framework to enable maximum information extraction from complex scenes by using all the photon pathways of captured light and leveraging light's multiple degrees of freedom. This framework will then be used to guide the development of new imaging hardware and software technologies. Those technologies will be tested against a challenge problem that calls for full 3D scene reconstruction from a single viewpoint—a rendering that today requires inputs from multiple viewpoints. Such an ability could enhance

situational awareness for troops, potentially allowing them to reconstruct, from a single vantage point, a complex scene including objects or people not visible by line-of-sight viewing.

Designing Complex, Dynamic Systems

DARPA's Complex Adaptive System Composition and Design Environment (CASCADE) program has a seemingly esoteric but ultimately practical goal: to advance and exploit novel mathematical techniques to gain a deeper understanding of system component interactions, a unified view of system behaviors and a formal language for composing and designing complex adaptive systems. Conventional modeling and design tools invoke static 'playbook' concepts that do not adequately represent the complexity of, say, an airborne system of systems with its constantly changing variables, such as enemy jamming, bad weather or loss of one or more aircraft. CASCADE aims to fundamentally change how systems are designed to enable real-time resilient response within dynamic, unexpected environments.

KEEPING DARPA VIGOROUS

The programs described above are a sampling of what engages DARPA every day, but of course DARPA is much more than a collection of programs. It is a team of about 200 extraordinary government employees whose collective energy not only propels the Agency but also invigorates scientists, engineers, mathematicians and others across the wide community with which we work—defense companies large and small, commercial startups and major firms, universities, government agencies and labs, and our close partners across DoD. It is a team that revels in the opportunity to attack pressing, nearly intractable problems—all in the context of public service.

DARPA's leadership takes seriously its responsibility to encourage the Agency's culture of high-risk, high-reward innovation and its ability to execute rapidly and effectively. Toward that end, we continue to experiment with better ways to reach new performers through, for example, the "EZ BAA" process launched by our Biological Technologies Office last year, which greatly simplifies the process by which performers can get on contract with DARPA for efforts of up to $750,000. The EZ BAA is especially helpful in reaching those unfamiliar with defense procurement.

We also continue to use our prize authorities, for which we are grateful. Prize authorities were crucial to the success of the DARPA Robotics Challenge, our

three-year push to accelerate progress in ground robotics for humanitarian assistance and disaster relief, which held its finals in California last summer. We are also using our prize authorities to run DARPA's Cyber Grand Challenge, which has been working to speed the development of automated cyber defense capabilities and will hold its final competition in August, when seven extremely talented teams will have their computers face off against one another at an event that is expected to draw thousands of spectators. In addition, we continue to use the prize mechanism for smaller efforts, such as last year's competition to model the spread of Chikungunya, a mosquito-borne infectious disease.

Of course, at the center of DARPA's success is an abiding commitment to identify, recruit and support excellent program managers—extraordinary individuals who are at the top of their fields and who are hungry for the opportunity to push the limits of their disciplines during their limited terms at DARPA. I am most grateful for the critical support this Subcommittee provided in authorizing the 1101 hiring mechanism, extending it, and in FY 2015 expanding DARPA's ability to use it. That authority has proven invaluable to our ability to attract some of the finest scientists, engineers and mathematicians to the important work of public service and national security. The 1101 experiment has now been running since 1999 and has clearly proven its benefits to DARPA and the Nation. After 16 years of annual uncertainty about its ongoing availability, we would appreciate your support to make this authority permanent.

DARPA'S BUDGET

The President's FY 2017 budget request for DARPA is $2.973 billion. This amount is the same as that requested for FY 2016 and $105 million more than the $2.868 billion appropriated for FY 2016. To put these numbers in context, from FY 2009 to FY 2013 DARPA's budget eroded significantly through a series of reductions, including the 8 percent across-the-board sequestration cut in FY 2013. The total reduction to DARPA's budget from FY 2009 to FY 2013 was 20 percent in real terms. With modest increases in FY 2014 and 2015 and a slight decrease for FY 2016, DARPA's budget has not fully recovered, but it has been more stable. I ask for your full support of the President's budget request for FY 2017 so that DARPA can continue to deliver on its vital mission.

CONCLUSION

As the programs I have highlighted today illustrate, DARPA's commitment to bolstering national security encompasses an extraordinary range of technologies and scientific domains, spanning dimensional scales from the atomic to the celestial, time scales from attoseconds to decades, spectral scales from radio waves to infrared to gamma rays, andbiological scales from genes and proteins to neurons and organs to infectious diseases and global health. Every day, the people of DARPA come to work to probe and push on those various frontiers. And despite the daunting security challenges around the globe that spur our work, the atmosphere within our agency is persistently one of excitement and even joy—a reflection of the fact that DARPA is obsessed not with problems but with solutions.

A highly functional, effective and spirited organization does not happen by accident. We within DARPA work at it constantly, drawing our inspiration from the amazing, ever-evolving world of technology and from a deep desire to serve our Nation. I and my colleagues at DARPA appreciate the ongoing support and trust this committee and subcommittee have bestowed upon DARPA. I am fully committed to ensuring that, just as past investments in DARPA helped secure our Nation by repeatedly bending the arc of technological history, so today's investments will give rise to capabilities that will protect our Nation and project our interests for many decades to come.

With that, I will be pleased to respond to your questions.