Statement by

Dr. Kaigham J. Gabriel

Deputy Director
Defense Advanced Research Projects Agency

Submitted to the

Subcommittee on Emerging Threats and Capabilities
United States House of Representatives

February 29, 2012

At DARPA, we are often asked to predict the future.

After all, since it was created in 1958, DARPA's singular mission has been to create and prevent strategic surprise. Simple. Clear. Direct.

It may appear that the best way to create strategic surprise is to predict what's next. Predict with great accuracy and as far as out as possible. We hunger to know what's next. To predict the future. But our hunger to predict is not matched by our ability to do so.

In 1964, Arthur C. Clarke, science fiction writer, inventor and futurist observed:

> "Trying to predict the future is a discouraging and hazardous occupation, because the prophet invariably falls between two chairs. If his predictions sound at all reasonable, you can be quite sure that in 20, or at most 50 years, the progress of science and technology has made him seem ridiculously conservative. On the other hand, if by some miracle, a prophet could describe the future exactly as it was going to take place, his predictions would sound so absurd, so far-fetched, that everybody would laugh him to scorn."

At DARPA, we believe it is not about predicting the future... it is about building it. Indeed, the technical visionaries at DARPA are not oracles—they are builders.

Chairman Thornberry, Ranking Member Langevin, Members of the Subcommittee, my name is Ken Gabriel. I am the Deputy Director of the Defense Advanced Research Projects Agency. I would like to highlight some of the accomplishments of the Agency over the last 12 months and, outline the challenges we see and our intentions for the coming year. The impact from some of our work will be felt years from now. Other work is contributing sooner and is in the fight today. Regardless of where in that spectrum we are, DARPA's work is underscored by a focus on building. Building capabilities and demonstrations at convincing scale that drive the advance of the underlying technologies and science. We innovate by building. We achieve our best, by building.

Building the future.

Some of the Agency's greatest contributions— things we now take for granted and as having been inevitable were, at their inception, often considered impossible. The Internet, stealth, UAVs for example, when first proposed were described by some as impractical, far-fetched, and risky.

But these seemingly impossible things were turned to the improbable and then to the inevitable by people with vision and determination to make their vision real. A determination to build. DARPA program managers have a hunger to succeed, a sense of urgency, and a commitment to the Nation's Security. For more than 50 years, the Agency has sought the Nation's best, given them the resources they need, and cleared the obstacles in their way.

The lifeblood of DARPA is the cadre of program managers and leadership executives that represent some of the best technical minds in the country. Professionals who put their careers in suspended animation in service to country. Accountable to the Agency, to the Department, and to our Warfighters, DARPA's program managers are drawn from academia, industry, non-profits, the Services, and laboratories and serve for a tour of 3 to 5 years. Program managers, office directors, the Director, and the Deputy Director; all change on a regular cadence. This practice results in roughly 25 percent annual starts and exits and ensures the Agency is current with existing and emerging technological trends, encourages a continual challenging of conventional approaches, and imparts an ethic of urgency.

One key continuing challenge for the Agency and, by extension, for the well-being of the Department of Defense is recruiting this talent to service. DARPA's ability to do so demands rapid, agile and efficient hiring. In the last 2.5 years the Agency has recruited more than 75 new program managers – this has been essential to many of our efforts including DARPA's significantly expanded cyber program and our big data efforts in support of operations in Afghanistan, among others. DARPA has demonstrated successful and responsible use of its hiring authorities. Indeed, the Agency has been at essentially present-day personnel levels since 1992 and has never exceeded the allocated top-line number of authorized full-time equivalents. Timelines for hiring within the Agency are short and match the cadence and tempo of tours reflected above. Simply put, we cannot undertake a 6-month or even a year-long hiring activity, as is common in government, for a technical subject matter expert critically needed to undertake efforts in response to a technological shift and with other competing career opportunities. Rather, we need to sustain an efficient and expedient engagement that is naturally always within the construct of fiscal, ethical, and legal responsibilities. This is not something we can afford to risk. Together we must protect it vigorously.

Our business practices are a vital part of building.

Execution is what allows the people at DARPA to build. To turn ideas into reality, the Agency must operate effectively with agility, speed, and technical and administrative integrity. DARPA executes a budget of nearly $3 billion as appropriated by Congress. It does so with approximately 120 program managers and a roughly equal number of Government support staff. Financial resources and lean business practices allow the Agency to pursue ideas that most dare not touch. And to do so quickly. There are no entitlements to programs or people, no captive laboratories, no immutable tenets. The Agency applies a "thoughtful ruthlessness" in its dogged pursuit of the best people, ideas, and output.

The breadth, urgency, and technical demands of DARPA programs are real. The innovative ideas the Agency pursues are fragile and fleeting, and the organization's business practices must be aligned with the speed and flexibility required to pursue those ideas. The authenticity of Defense applications demands an organization dedicated to excellence in execution through all levels of management, policies, and personnel. Indeed, in the face of such pressures, creativity requires heroic intellectual leaps not just from the technical side of the organization, but equally from the support side of the organization. DARPA has support offices dedicated to essential functions that enable the mission through innovative practices that mirror the technical innovations of the Agency.

In past years, Congressional oversight committees expressed concern that DARPA's financial execution was inadequate; specifically, that DARPA was not obligating a significant fraction of the money it had requested. These concerns resulted in budget cuts and rescissions, but, as well, obligation delays meant fewer resources at work for the Department. In our 2010 written testimony, we reported on the steps the Agency had taken to improve business process and the resulting, significant improvements in financial execution.

In 2011, we maintained our emphasis on responsible and efficient financial execution. At the end of September 2011, the Agency's obligation rate was 21 points higher (85 percent) than the 5-year average (64 percent) despite the delayed 2011 Appropriations signing. At the end of fiscal year 2011, the improved execution translated into more than $600 million in the performer community, working for the Department and Nation. Speed is part of the vibrancy of innovation and building. Better business practices are just better Government. It affects not only the performers, but the Agency too.

People come to DARPA not for careers in Government, but to serve. Over the decades, this cadre has consistently delivered. The list of historical achievements is well known, long, and includes stealth, the Internet, and UAVs. Today we are working on the production of vaccines from tobacco plants measured in days rather than months; prosthetics controlled directly by thoughts; and clean-slate, convergent approaches to defensive and offensive cyber security capabilities among many other innovations.

Discouraging the fear of failure.

Doing things that have never been done before, building the future, comes with risk. Risk of failure. As a Department, as a Nation, we must not forget that great accomplishments often had failure along the path. We cannot fear it.

The history of the Corona program and imaging satellites tells us that it took 13 launches over several years before the first images were collected. Thirteen. Each of the other 12 launches failed to collect a single image. No doubt, some at the time called them failures. But each of those 12 launches informed the next build and successively created the capability of imaging satellites from what seemed impossible, to just improbable and, eventually, inevitable. The first successful flight in 1960 covered 1.65 million square miles of Soviet territory—more than all earlier U-2 missions combined.

A more recent example is HTV-2, a DARPA program that is part of the Department's prompt global strike activities. HTV-2 seeks to travel at Mach 20 in an unmanned, boost-glide, maneuvering vehicle. The fastest high lift-to-drag ratio aircraft ever built. Mach 20. Twenty times the speed of sound. That means anywhere in the world in 60 minutes or less. Or New York to Los Angeles in 11 minutes and 20 seconds, with the surface of the vehicle at blast furnace temperatures: 3500 degrees F—the temperature of molten steel. We are essentially burning the airfoil as we fly it. It might seem impossible. It's not. It's just hard.

There have been two test flights to date. The first revealed an underestimation and simulation of aerodynamic effects in one of four variables needed for controlled hypersonic flight. The second flight demonstrated that we had fixed the aerodynamic control from the first flight, but precisely because we reached a different stage of the flight, we had 3 minutes of fully aerodynamically controlled flight at Mach 20. Although neither of the flights completed all elements of the tests, the two flights combined fielded the largest collection of flight-test assets assembled and yielded more aerodynamic and test measurement data at these hypersonic regimes than what has been collected in ground tests over the last 40 years. There's no way to learn to fly at Mach 20 unless you build… and fly.

From hypersonic flight to detecting overpressure during blasts, building remains important. A persistent, acute DoD need has been for a reliable, accurate and affordable method to detect and characterize traumatic brain injury or (TBI). We undertook basic and fundamental work in neuroscience and the effect of blasts on the fine structure that revealed the role of over pressure in TBI. Overpressure waves distinguish blast exposure from other types of causes of TBI (for example, sports injuries where acceleration and kinetic impact, but no overpressures are contributors).

Informed by this neuroscience work, DARPA launched a program to build, demonstrate, and evaluate a blast gauge that incorporated a pressure sensor, acceleration sensor, and recording electronics. Four versions of the gauge were built over the course of a year and for a total development cost of approximately $1 million. Each version building in the learnings—learnings from both the use and manufacturing of the earlier versions.

In partnership with the Army, the final version was fielded to an entire brigade of 841 warfighters, the 2nd Brigade, 4th Infantry Division in RC South over the course of six months—from August 2011 to February 2012. The initial units used to outfit the first brigade cost $85 per unit, 3 per warfighter per month of deployment for a total cost of $1.6M. But over time, informed by the building and shipping of over 16,000 units and incorporating improved manufacturing processes, the cost is now approximately $45 per unit, and the next brigade will be outfitted for $540,000.

At DARPA we plan for success, not failure. We don't seek, embrace, or celebrate failure. We learn from our failure, and we build future capabilities through persistence, focus, and informed trial. We don't encourage failure; we discourage the *fear* of failure.

The price of not building.

In the best of times, failure is difficult to endure. There is a hunger and need to be efficient. To husband our resources. In times of fiscal pressure that hunger is sharper.

The conventional wisdom and response for relief is to roadmap, coordinate and plan to better predict and better prepare. To slow our efforts so as to retire more risks, to build less often and thus lower costs. If we can improve our predictions, we can better plan for and build the systems needed.

The argument being, "We can't afford to fail." The trouble with this approach is that, out of balance, it fails to weigh the risks of not building. Because it is equally important not to lose sight of the companion worry: "What's the price of not building often and along shorter timelines?"

At DARPA we examined this fundamental argument through the lens of two parameters: per-system cost and total number of systems to be purchased. Across many different types of representative defense systems— air, land, and sea— over the last 2 to 3 decades, the analysis reveals a consistent and disturbing pattern.

Programs of record begin with a target per-system cost and total number of systems to be purchased. Over the course of a program, due to a variety of factors including financial constraints, technical risks and changing priorities, there is a steady *increase* in the per-system cost and a corresponding *decrease* in the total number of systems to be purchased.

For the systems we analyzed, with associated development and fielding times ranging from 14 to 30 years, the final number of systems purchased were typically *one-fourth* the original number of systems envisioned at the start of the programs.

The judgment of whether fielding one-fourth of the original number of systems is enough is not DARPA's. This pattern of increasing timelines to initial operational capability, increasing cost per unit delivered, and companion decrease in the number of units, is divergent with an increasingly dynamic threat environment. Our next step was to attempt to reveal what is causing the divergence.

Many people are familiar with Norm Augustine's chart that shows the extrapolated cost of a fighter aircraft intersecting with the Defense budget, such that sometime in 2054 the entire Defense budget will be required to buy one aircraft.

Further, given the pace of global technological development and access, we can no longer afford the *time* it takes us to build Defense systems. In DARPA's 2010 and 2011 written testimony, we highlighted and described the Agency's advanced manufacturing initiative, with the focus on reducing and controlling for time. But it is not simply the argument that time is money. As a Department, we are at a juncture where not only the increasing cost but the increasing time it takes us to develop defense systems is a vulnerability in and of itself.

In the past, defense technology could be relied on to be ahead of civil or commercial technology. Defense technology drove commercial technology and the defense industry was often an early adopter and customer of new technologies. And in a few unique areas, defense will remain ahead of commercial capabilities. But the number of these areas is decreasing.

In the last 2 decades, this long-standing precedent has begun to reverse, and commercial technology has begun to outstrip defense technology. This is perhaps felt most acutely in cybersecurity and the consumer electronics products and services that have fundamentally changed the way we connect and interact with the world and each other.

Vulnerabilities created by commercial technologies.

Unintentionally, and without malice, commercial consumer electronics has created vulnerabilities by enabling sensors, computing, imaging, and communications capabilities that as recently as 15 years ago, were the exclusive domain of military systems. These capabilities now are in the hands of hundreds of millions of people around the world and in use every day.

The effect of these commercial capabilities on Defense and National Security may be seen in the impact of these trends on electronic warfare (EW) systems and anti-access and area denial (A2AD). EW: an area of historic advantage to the US military; and A2AD: an area of increasing concern in several strategic regions of the globe.

This is not an abstract vulnerability. We have not enjoyed spectrum dominance since about 1997. Up until then, our EW systems could both detect and respond effectively to EW threats directed at us. In the last 15 or so years, however, that has ceased to be true. In both waveform complexity and carrier frequency, adversaries have moved to operating regimes currently beyond the capabilities of our systems.

What we find are three principal reasons why it has been possible to apply commercially available electronic capabilities to produce military-grade EW systems.

First, as microelectronic devices continue to shrink in size, they are, perhaps counter intuitively, also improving in performance. For example, smaller microelectronic devices are able to switch faster and, thus, operate at higher frequencies. This means that specialized microelectronic devices produced for DoD are now matched or nearly matched in performance to standard silicon-based microelectronics commercially available from multiple, global sources.

Second, custom signal processing chips that took 2 to 3 years to develop and required chip designers, sophisticated design, and simulation tools along with chip fabrication facilities are increasingly being replaced by programmable chips or field-programmable gate arrays (FPGAs). Unlike custom signal processing chips that have their specific function fixed at the time of fabrication, FPGAs can be programmed, and reprogrammed, like software, *after* fabrication. This means that developers can cut as much as 18 months off development schedules, from 3 to 4 years to as little as 1.5 years.

Finally, the demand created by the global, mobile communications industry has led to a global manufacturing capacity and economic efficiencies that deliver the above capabilities at ever decreasing prices.

EW was once the province of a few peer-adversaries. It is now possible to purchase commercial off-the-shelf (COTS) components for more than 90 percent of the electronics needed in an EW system. This has reduced the barriers to developing, producing, and fielding such systems to within the capabilities of many nation states and non-state actors.

And because of the improved performance of commercially available, programmable microelectronics, nearly a dozen countries are now producing EW system variants and new versions at a much faster cadence than we have; from a pace of a new system every 5 to 10 years 2 decades ago, to one every 1.5 years today. This means that our conventional approaches no longer afford us a time or capability advantage.   Increasingly, our conventional approaches are divergent with the threat.

These insights led us to new investments that leverage COTS technology where it makes sense to, counter COTS where we need to, and transcend COTS where practical.

Leveraging COTS.

If a commercial computer chip is fast enough to accomplish a task in a US military system, there is no point to designing an alternative; just use what is available. This does not imply equivalent capability at the system level. Namely, we are not doomed to an even playing field just because we are using the same processor chip as an adversary. We can make a network of such chips to overcome the adversary's system. Better algorithms tightly integrated with the hardware, and improved cooling to wring more performance from each chip, are two examples where technological advances would allow us to prevail even when we are all using the same basic technology.

Countering COTS; alternatives to GPS as an example.

We use global positioning system (GPS) because it is cheap and easy. It is COTS for us – most of our precision-guided munitions capability, as well as timing for our command and control systems, have become dependent on GPS. The adversary knows this and has aggressively sought means to counter our dependency on GPS. Jammers and commercially driven spectrum compression may threaten our ability to use GPS in areas denied. Attempts to make GPS receivers that can survive that jamming is impractical and not convergent with the threat. GPS signals are inherently weak. The ease with which GPS signals are jammed or spoofed motivate developments of development of alternative position, navigation, and timing approaches that are not dependent on GPS alone.

An example of how we might counter COTS is to recognize that GPS is just one way of providing positioning, navigation, and timing data.   But it is not the only way. We might carry our own navigation system. The same trends in COTS advances, used to build alternative navigation guidance systems such as highly integrated, inexpensive, low power accelerometers and gyros, may enable the DoD to accomplish its mission even when GPS is denied. Our analysis revealed that extending the performance of today's inertial guidance systems by a factor of 20—from roughly 1 minute to 18 minutes, will permit 98 percent of our GPS-dependent weapons to operate at GPS accuracy during their mission duration without a GPS signal.

Transcending COTS.

COTS electronics is a formidable source of new, high performance technology, but it has inherent limitations. The main one is economics– industry is motivated by the profit incentive, and modern electronics is extremely expensive to design and produce in small volumes. This highly nonlinear effect of high volume manufacturing is why the extremely complex technology inside cell phones appears to be so cheap.

This opens a window of opportunity for the US military anywhere that product unit volumes will be low, COTS electronics will be unavailable. Very high power transmit/receive modules for radars and radios, for example, are simply unnecessary in the COTS space, so the Military must design and produce its own. Although this performance advantage will come with a cost greater than commercial products, this means the United States will enjoy a technical lead over any potential adversary who cannot invest and do likewise.

Operational vice intelligence capabilities in cybersecurity.

In cybersecurity, we have the area that most highlights the danger of taking too long to build. The shelflife of cybersecurity systems and capabilities is sometimes measured in days. Thus, to a greater degree than in other areas of defense, cybersecurity solutions require that we develop the ability to build quickly, at scale, and over a broad range of capabilities. This is true for both offensive and defensive capabilities.

DARPA's role in the creation of the Internet means we were party to the intense opportunities it created and share in the intense responsibility of protecting it. We should emphasize that national policymakers, not DARPA, will determine how cyber capabilities will be employed to protect and defend National Security interests. But the Agency has a special responsibility to explore the outer boundaries of such capabilities that the United States is well prepared for future challenges.

To date, there has been much focus on increasing our defensive capabilities. To be sure, the list of needed capabilities is long. Our networks may be safer than they were, but systems are often easily penetrated, accounts are routinely hacked, intellectual property and sensitive information are compromised, and the supply chain is not secure. And because computers are embedded in nearly all our systems—cyber attack cannot be regarded as a threat only to our networks and information—but rather to all our physical systems as well.

Protecting cyberspace and the Nation requires both significantly enhanced defensive and offensive cyber capabilities; capabilities across the full spectrum of the conflict. Of note, our Intelligence Community has significant cyber capabilities, but the are geared predominantly to intelligence tasks. The tasks required for Defense purposes are sufficiently different that we cannot simply scale our intelligence cyber capabilities and adequately serve the needs of the Department of Defense. Rather we need cyber options that can be executed at the speed, scale, and pace of our military kinetic options with comparable predicted outcomes.

Modern warfare demands the effective use of cyber, kinetic, and combined cyber and kinetic means. That will happen only if cyber capabilities are at scales and speeds matched to our kinetic options.

Informed by these insights and with a willingness to accept our responsibility to contribute, we assessed that DARPA has a significant role to play. We recruited an expert cyber team of individuals from diverse experiences including the "white hat" hacker community, academia, labs and nonprofits, major commercial companies, in addition to the Defense and Intelligence Communities.

We launched several programs, increased the level of activities in others, and closed some out. Our cyber efforts are designed to create the capabilities needed for military missions. We need more options. We need more speed and scale. We need approaches that match the diversity, dynamic range, and operational tempo of DoD activities. This cannot be achieved by simply doing more of what we've been doing or by increasing our intelligence-oriented cyber capabilities.

Examples include programs such as Clean-Slate design of Resilient, Adaptive, Secure Hosts or CRASH, which takes its inspiration from the defensive mechanisms of biological systems and seeks to develop cybersecurity technologies by radically rethinking basic hardware and systems designs. And PROgramming Computation on EncryptEd DATA or PROCEED, which is a big reach program motivated by recent breakthroughs in what is called fully homomorphic encryption, which could fundamentally change the nature of assured computations on untrusted hardware. If successful, PROCEED puts cybersecurity into an encryption realm, a realm that requires state-level computational resources.

The Cyber Fast Track program recognizes an untapped pool of experts and innovators who could contribute, if we provide a path. That path matches both their execution and the shelflife of cybersecurity products. In the last 7 months, more than 100 proposals were received by Cyber Fast Track, and 32 awards were made. Just as important, the average time from receipt of proposal to award is 7 days. We note that the process and contracting mechanism rigorously meets DoD regulations for competition and awards; we need not be slow to be fair, ethical, or prudent. Eighty-four percent of these small companies and performers have never done business with the Government before, expanding the number and diversity of talent contributing to the Nation's cybersecurity.

Since 2009, DARPA has steadily increased its cyber research. Our cyber research funding is increasing from $228 million in FY2012 to $246 million in FY2013. And over the next five years, our proposed investment in cyber research will grow steadily from 8 percent to 12 percent of topline.

We are also shifting our investments to activities that promise more convergence with the threat that recognize the unique needs of the Department of Defense. To this end, in the coming years, DARPA will focus an increasing portion of our cyber research on the investigation of offensive capabilities to address military-specific needs.

We began these efforts on our own. But part of the growth in our resource commitment beginning in 2012 and extending through 2017, is at the hand of senior leaders in the Department, who added $500 million over 5 years for clean-slate, convergent cyber research at DARPA.

DARPA's engagement in cyber is not new. This expanded effort builds on an existing foundation and continuing contributions to cyber. Indeed, past DARPA-developed technologies are widely prevalent in military, intelligence, and commercial use today. But there is still much to do.

DARPA activities are part of a larger whole within National Security at the National Security Agency , the newly formed CYBERCOMMAND, the Services, the private sector, universities, nonprofits and, as appropriate, the Department of Homeland Security.

Clearly, the challenges of cyberspace require the concerted efforts of many. Indeed, we all must be protectors of and operate within cyberspace.

And these challenges also demand the involvement of technical experts at unprecedented levels. We expect that part of our responsibility will be in advisory roles during the formation of policy and legal frameworks, because new policies and laws—domestic and international—must be executable, enforceable, and sustainable.

To be of use, such policies and laws will demand evaluation and adjustment on timescales that correspond to the dynamic nature and compressed evolutionary timescales of advances in cyberspace. We'll have to move faster than we are accustomed to. We'll need the tools and guidance to do so.

Discomfort and strategic surprise.

Some of these observations feel uncomfortable. Even to us. Our responsibility, however, is to the uncomfortable. It is the Agency's singular mission to identify divergences and the threats and opportunities they represent. These are the seeds of strategic surprise.

We need approaches that are convergent with the challenges and deliver systems and solutions on timescales and with agilities that match operational needs.

In this time of fiscal constraint, we are committed to doing our part. But this does not mean that we lose our nerve for building.

Thank you.