GETTING INNOVATION RIGHT

Edited by Mona Dreicer

Center for Global Security Research
Lawrence Livermore National Laboratory
September 2019

GETTING INNOVATION RIGHT

Edited by Mona Dreicer

Table of Contents

Preface: Getting Innovation Right in the Strategy for Long-Term Competition

As we celebrate the fiftieth anniversary of the Apollo 11 moon landing, the importance of science and technology advancement and innovation is front and center. The role of innovation is easily recognized—it changes, improves and, in many cases, replaces and makes obsolete the tools used in our daily lives. Innovation is shaped by the mission, degree of competition, and urgency to find a "solution." Notably, often it is no longer shaped by the strategies of a few governments. The commercial and global aspects of the private sector have vastly complicated the ability to direct innovation towards good public purpose and not only for individual gain.

In the national security environment, innovation has been recognized as a key factor in the ending of World War II and influenced the outcome of the Cold War. The strategy of the third offset, announced in 2015, was to use innovation to sustain and advance U.S. military dominance. The 2018 National Defense Strategy (NDS) highlights the shift to an environment of great power rivalry, thus requiring the refocus of U.S. national defense strategies:

> *We are facing increased global disorder, characterized by decline in the long-standing rules-based international order—creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security that is affected by rapid technological advances.*

The NDS calls for the creation and maintenance of a "National Security Innovation Base" that "effectively supports Department operations and sustains security and solvency." A congressionally empowered, bipartisan NDS Commission undertook a review of the NDS. They outlined clear areas of need, including the aggressive pursuit of technological innovation and introduction of these innovations to position the U.S. military for success.

The renewed prominence of ***innovation*** as a ***solution*** raises many challenges. What does it mean to get innovation right? Can major powers "out-innovate" their rivals? Bureaucracies traditionally struggle with innovation, so how can new mindsets, partnerships, and processes be initiated and implemented?

The Center for Global Security Research at Lawrence Livermore National Laboratory hosted a workshop to better understand the relationship between defense strategy and emerging innovation. The goal was to uncover processes, whether public, private, or collaborative, that could foster innovation to bolster national security, as well as identify which practices impede developments necessary to outcompete adversaries.

The following key questions guided the discussion:

1. What is required to out-innovate major power adversaries?
2. What goals and metrics should guide innovation strategies?
3. Does the strategy for S&T innovation adequately address all the military domains where the major powers compete?
4. Does the defense strategy ensure the innovation needed in strategic and operational concepts, organizations, and processes?
5. Are there useful lessons for innovation from past defense-reform efforts?

This workshop brought together participants from across the policy, military, and technical communities. Sixty-three participants addressed topics concerning U.S. innovation strategy and interdepartmental initiatives, adversaries and innovation, drivers of technological strategy, private–public collaboration, and ally innovation—and in particular, to consider the Department of Energy's National Nuclear Security Administration contributions to the larger context. The conversation included obstacles to effective innovative policy and how any long-term strategy must adjust accordingly to ensure innovative.

After two days of discussion, we asked a few contributors to summarize their remarks for this publication. *The views expressed are their personal views and should not be attributed to Center for Global Security Research, Lawrence Livermore National Laboratory, or the U.S. Government*. A more expansive workshop summary is available at the CGSR website, https://cgsr.llnl.gov/content/assets/docs/CGSR-Innovation-Workshop-APR2019-Summary.pdf

Mona Dreicer
September 2019

U.S. Defense Strategy and the Innovation Imperative

Charles Lutes

The point of departure for any contemporary analysis of the means and ends of innovation for national security should be the 2018 National Defense Strategy (NDS).[1] The strategy describes a complex and dynamic security environment marked primarily by a renewal of rivalry among the major powers and with it new forms of strategic competition and new forms of strategic conflict. Among the dynamic elements it highlights is the technological dimension: strategic competition with Russia and China is characterized by a seemingly relentless drive to develop new technologies—advanced computing, big data analytics, artificial intelligence, autonomy, directed energy, hypersonics, and biotechnology. Multiple simultaneous technological revolutions are likely to significantly impact the character of war. The competitor that best harnesses these technologies will have the advantage in fighting and winning the wars of the future. The NDS exhorts the nation to foster a competitive mindset and emphasizes the need to "out-think, out-maneuver, out-partner, and out-innovate" our competitors and potential adversaries.

It is not surprising that the NDS focuses on innovation as a key to out-competing adversaries during a period of rapid technological change. At the same time, the NDS hints that technological innovation is a necessary, but not sufficient condition, for out-innovating the competition. As technology advances, the nation's military must also seek to innovate its operational concepts and doctrine, as well as its organizations. Each is explored below.

Technological Innovation

At first blush, today's strategic competition might remind us of the beginning of the Cold War era and the technological competition that ensued. During that time, national security imperatives were the fuel for this nation's innovation engine. Put another way, during the Cold War, *strategic competition drove technological innovation*. Today the reverse may be true: *technological innovation may drive strategic competition.*

On the nuclear front alone, consider the innovative period between 1945–1965 during which the United States

- developed, produced and fielded a widely diverse arsenal of over 31,000 nuclear weapons;

1 *Summary of the 2018 National Defense Strategy of the United States of America*. Department of Defense, Washington United States, 2018.

- developed the jet engine and fielded thousands of jet fighters and bombers, many capable of delivering nuclear weapons;
- developed and deployed nuclear-tipped ICBMs; and
- developed and deployed submarine-launched nuclear ballistic missiles.

By contrast, in the two-decades from 2015–2035, the United States will struggle to recapitalize its nuclear triad with roughly the same type of capabilities in delivery systems and a vastly more limited nuclear arsenal in both numbers and diversity. However, during the same period, advances in hypersonics, directed energy, and artificial intelligence may drive the strategic competition in unforeseen directions.

Consider the case of artificial intelligence (AI). China was thought to have had a "Sputnik moment" in 2017 when Go grand-master Kei Jie was defeated by an AI algorithm called Alpha Go, developed by Google DeepMind. Defeat in its national game spurred the Chinese government to declare a policy of becoming the world leader in AI by 2030—a "moon shot" similar to President Kennedy's declaration in 1962. The Chinese have three big advantages that suggest they can achieve that goal: 1) a ready source of massive data sets relatively unencumbered by privacy concerns; 2) an entrepreneurial spirit in its AI workforce, which is shedding its copycat mentality for true innovative capacity; and 3) government support at all levels, including significant investment at state and local levels.[2]

By contrast, the U.S. has been late in providing policy guidance to advance AI, publishing an executive order in February of 2019 exhorting government agencies to "explore collaboration with non-federal entities." The challenge is that innovation in AI occurs largely in the private sector and without federal funding, providing few government levers for driving AI to support national security priorities. Recently, the Defense Advanced Research Projects Agency (DARPA) announced a significant increase in DOD investment in AI research, adding approximately $2 billion in investment over five years to its current average yearly spending of $2 billion. By contrast, the city of Shanghai alone expects to invest $15 billion over 10 years in AI research.

Granted, these metrics are inputs that do not provide adequate measures of the progress made by each country in AI innovation. Development of useful metrics would be an important first step in understanding the nature of technological change in the context of strategic competition.

Innovation in Operational Concepts and Doctrine

The NDS suggests the need to "evolve innovative operational concepts" and recognizes that modernization is not solely about technological change. It emphasizes the need to anticipate the implications of new technologies on the way we fight and

2 Lee, Kai-Fu. *AI Superpowers: China, Silicon Valley, and the New World Order*. Houghton Mifflin Harcourt (2018).

how adversaries will employ new technologies to defeat us. Yet the National Defense Strategy Commission[3] was rightfully skeptical of the Department's ability to innovate in its operational designs.

Our competitors have clearly been focusing on innovation in their operational concepts. The idea of gray-zone warfare that advances our adversaries' aims without significant U.S. response is one such example. Russia has also been innovating at the other end of the spectrum, using nuclear force as an element of coercion while considering forms of escalation. The U.S. has been slow to respond to these innovations, preferring instead to hone its advantages in conventional warfare. What seems to be clear is that future warfare will be conducted across the entire spectrum and the U.S. is ill prepared to compete at the low and high ends of that spectrum.

In my view, the emphasis on strategic competition in the NDS obscures the importance of operational concepts in future war. Consider the case of hypersonic-technology development. The U.S. has been slow to leverage its decades advantage in this technology, and now that Russia and China have begun testing and fielding hypersonics capabilities, we are just now waking to a potential "hypersonic gap." Michael Griffin, undersecretary of defense for research and engineering, has stated that the U.S. will have "thousands" of hypersonic weapons. Yet no one has articulated a concept of operations for these weapons and, in truth, there are no programs of record in any of the services for a fielded hypersonic capability. It seems the initial concept is to compete for the sake of competition with little regard for how hypersonics might actually improve our operational advantage.

Organizational Innovation

The NDS recognizes that the current processes of the Department are not responsive to need and articulates the desire to "deliver performance at the speed of relevance." Delivering performance means eliminating outdated processes and structures and bringing in the best insights from the business world. The NDS further states that the Department will "organize for innovation" by adapting those structures that best support the joint force.

While the instinct is correct, there is no real roadmap for achieving this vision, and the reality on the ground is quite chaotic. The NDS Commission suggests that the emphasis for defense programs has historically been focused more on making the acquisition system function more smoothly than optimizing for innovation and technological breakthroughs. This has created a condition where innovation takes place largely outside the government, making it increasingly difficult for DOD to access new technologies quickly, if at all. To get around this problem, we have witnessed the

3 National Defense Strategy Commission. *Providing for the Common Defense: The Assessments and Recommendations of the National Defense Strategy Commission*. United States Institute of Peace (2018).

flowering of a multitude of new organizations planted on top of the rotted wood of the DOD acquisition system.

The Schumpeterian theory of economic innovation introduces the notion of creative destruction—a process of industrial mutation that destroys sclerotic organizational structures and replaces them with new, more efficient forms. Unfortunately, creative destruction rarely occurs in government. New structures appear, but old ones never die, nor do they fade away. Acronyms such as DIU, SCO, RCO, SOFWERX, AFWERX, and JAIC have entered the Defense innovation ecosystem, without a guiding vision or a common understanding of how these organizations might function or integrate with the DOD acquisition system.

Consider the case of space. Which organization will drive innovation in space capabilities: a retooled Space and Missile Systems Center (SMC 2.0), Space Rapid Capabilities Office, or the Space Development Agency? And which organization will drive innovation in operational concepts: Space Command, Space Force, or the legacy services and NRO? A guiding vision for the national space enterprise should clearly articulate how these organizations should fit together.

Conclusion

The National Defense Strategy is to be commended for recognizing the importance of innovation in an era of strategic competition. But the vision it has set out is incomplete. A further articulation and roadmap will be required to drive the organizational innovation, innovation in operational concepts and doctrine, and technical innovation required to compete successfully. The record since the NDS was published suggests that the imperative for change has yet to take hold in the Department of Defense. At its core, innovation in these areas requires cultural change. Consistent and sustained leadership attention will be necessary to attain the grand vision set out by the National Defense Strategy.

Getting Focused: Innovation in a 21st Century Context

Robert Kehler

We live in a time of extraordinary change. From the way we communicate and travel, to the medical care we receive, to the way we shop, to the threats we face, change is occurring all around us. But change isn't new. Those of us who have been around for a while (let's say those who are part of the post-World War II baby boom and a bit beyond) have seen tremendous technological advances and real existential threats to our national survival before. So, why all the concern today?

I believe there are profound differences today that make this time unique in terms of challenges and opportunities. The key issue is how to leverage the opportunities before the challenges overtake us. Innovation is a part of the solution, but only when we understand how to focus, capture, and apply innovation effectively to the most difficult problems. Understanding the key drivers of change (environment, need, opportunity) and how to balance them is an important precursor to focusing innovation in a meaningful way.

Environment Drives Change

History confirms that our environment drives change (and vice versa). Every epoch can claim environmental factors that drove change. In my view, the era in which we live can claim these:

- ***Tremendous speed*** (not velocity, which has a direction vector)—Everything seems to be going faster, and time does not appear to be on our side. Policy is lagging behind technology and the gap is getting wider by the day. No one relaxes and everyone demands more while they move at a frantic pace.

- ***Unprecedented access***—Places, people, and information are accessible in hours, minutes, seconds, and milliseconds. My generation didn't "shrink the kids"; my generation shrank the world.

- ***Ultra-high volume*** (amount and decibels)—Information, data, and conversation are all at extreme volume levels. Everyone is drowning (in information) or shouting (usually at one another) and it is almost impossible to tell the difference between urgent and important.

- ***Fiendish complexity***—Law, finances, relationships, systems, and programs all seem difficult (maybe impossible) to understand, and the interrelationships among and between them often create new and unintended consequences when one or another factor is changed. Out of necessity, we must rely on a relative handful of highly specialized “experts” to help us decipher this complexity.

- ***Sharp divisions***—Everyone has picked sides and everything is characterized as win versus lose.

- ***New vulnerabilities***—Someone can enter your home, business, or secure area and steal your most important stuff—and never physically be there. Equally concerning, an insider can do that while authorized to be there—by you—because you trust him. Here’s another troubling characteristic of the 21st century environment. While it isn’t new that the U.S. homeland is at risk from potential adversaries, it is new that the homeland is at risk below the nuclear threshold, from conventional and cyber weapons, and therefore from a larger pool of potential adversaries.

- ***Decisive consequences***—Business decisions, personal behavior, and innocent mistakes are instantly and publicly debated and judged. This can make organizations and leaders far less tolerant of risk-taking at the very time when tolerating a higher level of risk is necessary to foster innovation.

Need Drives Change

The government often struggles to clearly describe what it needs (requirement), how it intends to use it (operating concept), or why (strategy). Worse, big-picture needs (usually integrated or mission-level capabilities) cited by senior civilian and military leaders don’t always translate into program needs (usually a piece of what the senior leaders are talking about) cited by the acquisition system and Congress. The resulting miscommunication often results in frustration with “lack of innovation” as the presumed cause. Over the last several years, senior Department of Defense (DOD) leaders have spoken forcefully of these needs:

- ***More lethality***—Focus on warfighting effectiveness and benefits (for example, longer range, more tooth vs tail, and higher readiness rates). Getting more out of what has already been purchased is a further hallmark of this need.

- ***Rapid technology infusion***—Take advantage of the rapid pace of technology within operationally relevant timeframes. Open system architectures and block upgrade strategies are frequently mentioned in these conversations.

- ***Effective resilience and security***—Mission (or architectural), network, and platform resiliency that results in warfighting resilience. Less emphasis on fielding systems (especially IT networks) that can totally defeat threats and more on systems that can function despite the threat.

- ***Better integration***—Across domains, platforms, and missions

- ***Game-changing innovation***—The equivalent of nuclear weapons, night vision, precision strike, stealth capabilities, etc., that will leap the U.S. military ahead of adversaries

- ***More speed***—Speed is the new mantra across the DOD. There is a sense that the U.S. has fallen behind and adversaries are outpacing us. At some level speed has become an independent virtue without answering the key questions, what has to go fast and how fast must it go?

- ***Technically capable people***—Recruit and retain high-end talent while competing for the best and brightest

Opportunity Drives Change

This is a time of great opportunity if we can sort through the noise and focus on the end results. One only has to look at the endless stream of technological breakthroughs and the entrepreneurial spirit that produced them to recognize the innovative benefits that are available to the DOD. In fact, there is no shortage of desire from DOD to embrace opportunities of these kinds:

- ***Commercial capabilities***—Commercial companies are offering significant capabilities faster and at lower costs than traditional government acquisition. Prime examples are found in space-related capabilities like launch, earth observation, and communications. Others are found in information technology, applications, and data management.

- ***Better partnerships***—New technologies and capabilities are available via partnerships with existing and new industry, allied, and governmental partners. Allies can bring significant capabilities to coalition operations.

- ***Consumer-driven technology***—In many cases, government is no longer leading the demand or the investment for advances in materials, artificial intelligence, quantum and other advanced computing, data management and security, and autonomous vehicles and drones.

So, how do we proceed? The environment is forcing change, senior civilian and military leaders are demanding change, and opportunities exist to produce change. But something seems to be holding us back. The DOD has spent much time and effort on fostering innovation with new organizations (e.g., the Defense Innovation Unit) and increased commitment from existing organizations (e.g., Defense Advanced Research Projects Agency [DARPA], national labs, and service labs), yet leaders still lament a lack of rapid progress.

From my perspective, the problem is not a lack of innovators or innovation. The United States still leads the world in many areas of academic, entrepreneurial, and industrial innovation. Rather, the problem is that we lack the ability to harness innovation effectively. This is so for two primary reasons.

First, there is a major incompatibility between requirements-based acquisition (such as an F-35) and opportunity-based acquisition (e.g., an iPhone). While innovation finds its way into the F-35, it certainly doesn't happen with the same speed and agility as in the iPhone. The philosophy, processes, mechanisms, and time scales that led to these two products are fundamentally (and maybe irreconcilably) different. This problem will continue to impede progress until a way is found to offer incentives and entry points for opportunity (innovation) into the requirements-based DOD acquisition process. I have heard directly from companies who believe they have innovative ideas or products but have been rejected or shuttled among a variety of offices because there is no "innovation" doorway for them to enter. In some cases, they just don't know how to approach the government.

Second, the DOD doesn't "ask" for innovation; it asks for programs. Senior leaders tell industry what they need, but they don't ask for it in acquisition terms. So, while the Air Force Chief of Staff repeatedly states that his service needs multidomain command and control, industry is delivering individual, not integrated, programs. Again, in my experience, large corporations in the defense sector usually produce programs that span a range of DOD missions, domains, and services, but they don't routinely *propose* integrated solutions because the DOD doesn't ask for them in acquisition terms.

Perhaps a useful model for success is the collaborative effort among science, academia, industry, and the military that led to digital computing, information technology, and the deployment of the Semi-Automatic Ground Environment (SAGE) system in the 1950s. This system for real-time continental air defense was fueled by innovation and linked sensors, shooters, and command and control into a single integrated activity—exactly what the Air Chief is asking for across domains today.

To meet the challenges of today and tomorrow will require us to routinely and effectively harness the engines of innovation. It's possible, but not until ways are found to marry innovation with a requirements-based DOD acquisition process that begins with a document instead of an idea. A recipe for success just might be found in SAGE.

“Innovating” Versus “Out-Innovating”: Innovation as a Form of Strategic Competition

Paul Bernstein

When it comes to innovation for national security, the 2018 National Defense Strategy (NDS) sets out a very specific goal. It is not merely to compete with ourselves to improve national competitiveness. Rather, it is to compete with others—principally with our major power adversaries, who are highly motivated and focused on the challenge of besting the United States and its allies in long-term competition. What are the particular requirements of a U.S. innovation strategy aimed at out-competing major power adversaries? Seven are discussed briefly here.

First, we need realistic, strategy-driven, measurable goals. These are difficult to find in available strategy documents. To some degree, innovation can be organized around general technology challenges that are widely viewed as critical, regardless of specific strategic or operational imperatives. But such an enterprise must at some point be tailored to support the goals of strategic-operational competition. Some would argue that we are competing, and therefore must innovate, to achieve dominance or comprehensive overmatch of great power adversaries. This is a clear goal, but highly ambitious and not strongly linked to the warfighting challenges facing the joint force. Others would argue that innovation should be shaped by a more realistic goal of deterring great power aggression. Here, the challenge is to define which specific threats should define the pace and direction of innovation. One way to answer this question is to focus on deterring the types of regional aggression that appear most likely to pose the hardest challenge to the joint force: campaigns in which adversaries seek to exploit advantages in geography, political stakes, and certain types of capabilities (e.g., anti-access/area denial and nonstrategic nuclear weapons) to achieve quick victories against the United States and its allies.

Still others would argue for deconstructing the problem further to define a more tailored set of tasks for defense innovation. This approach would organize innovation strategies around specific operational challenges that require solutions not likely to emerge from traditional approaches (see item 3 below). These operational challenges are, by definition, posed by adversary capabilities and concepts and overcoming them is key, not just to operational success, but to shaping adversary perceptions of U.S. purpose and resolve.

Specific operational challenges around which to organize innovation efforts are provided only in the classified portion of the 2018 National Defense Strategy (NDS). The NDS Commission report *(Providing for the Common Defense)* defines a set of “core operational challenges” that may be a useful point of departure for unclassified discussion. These include,

- Protecting forward bases of operation
- Rapidly reinforcing and sustaining forces engaged forward
- Assuring information systems and conducting effective information operations
- Defeating anti-access, area-denial threats
- Deterring and, if necessary, defeating the use of nuclear and other strategic weapons in ways that fall short of justifying a large-scale nuclear response
- Enhancing the capability and survivability of space systems and supporting infrastructure
- Developing an interoperable joint command, control, communications, computer, intelligence, surveillance, and reconnaissance architecture that supports future warfare.[4]

Interestingly, these challenges closely resemble the operational goals that defined defense transformation initiatives in the 2001 Quadrennial Defense Review (QDR).[5] This approach helps to bound the problem and lends itself to more concrete measures of success.

Second, we need a sense of urgency and the means to accurately assess what others are doing. Russia and China are committed to developing leading-edge military technologies and fielding "high-tech forces" in part because they see U.S. dominance as an existential threat. They are highly motivated. It is not clear the United States is as sharply motivated, which creates the potential for a focus or commitment gap. Closing any such gap is something leadership should pay attention to; otherwise it may take a crisis or a military failure to generate the necessary sense of urgency.

A clear understanding of what adversaries are trying to accomplish through their own efforts towards innovation is vitally important. This requires a robust capability for intelligence and operational "diagnostics." Russia and China clearly are making progress, though measuring this progress is not always easy. Particularly in the case of China, which is less transparent, it is important to realistically assess reported breakthroughs. There is a tendency to be too credulous about Chinese claims. One factor contributing to Chinese opacity, paradoxically, is the People's Liberation Party's (PLA's) lack of operational experience, which requires China to "learn without fighting." By contrast, Russia's various military adventures have allowed it to test concept and capability innovation in real operating conditions. Most recently, Syria has been a powerful testing ground that is shaping technology and operations.

Third, we need an integrated approach. A dynamic approach to innovating for operational advantage requires taking account of all forms of innovation, determining the appropriate mix for the types of conflicts the armed forces are likely to engage in and the specific operational challenges they will need to overcome. Innovation

4 National Defense Strategy Commission. *Providing for the Common Defense: The Assessments and Recommendations of the National Defense Strategy Commission*. United States Institute of Peace (2018).

5 *Quadrennial Defense Review Report*, Department of Defense (September 30, 2001).

encompasses not only technology but also operational concepts and organization/process. Military innovation and transformation leaders have long argued against an overemphasis on technology at the expense of other factors. Typically it is some combination of technology, concepts, and organization that provides a basis for breakthroughs. Often we are reminded of this when an adversary demonstrates it.

High-end regional war is generally the default lens through which we view requirements for innovation and it may be true that the bulk of defense innovation will be directed at this problem. But the spectrum of conflict also includes hybrid warfare (a mix of regular and irregular armed conflict) and coercive activities short of armed conflict ("political warfare")—modes of conflict that are not entirely new, but whose contemporary manifestations are indeed novel and for which the United States generally seems poorly prepared. We cannot dismiss the requirements for innovation in these aspects of great power competition, not least because they may lead us down pathways much different from those shaped by the demands of high-end regional war.

The following matrix may be useful as a very simple way to visualize the "battlespace" for innovation.

TYPE OF WARFARE	TYPE OF INNOVATION		
	TECHNOLOGY	OP CONCEPTS	ORG / PROCESS
HIGH-END REGIONAL			
HYBRID			
POLITICAL			

It is worth noting here that political warfare may be somewhat anomalous when considered as an arena of great power competition. In this domain, the goal of the United States and its partners is not to out-innovate adversaries so as to build the more advanced toolkit for political subversion, social division, economic warfare, and coercion. Rather, the West's goal is to greatly improve the ability of liberal states to reduce their vulnerability to such strategies and actively resist them. This is a somewhat different context for innovation, but an important one given the strategic stakes.

To better understand the potential dimensions of a high-end regional war, the following matrix arrays the types of innovation against the seven core operational challenges identified by the NDS Commission.[6]

6 National Defense Strategy Commission. P*roviding for the Common Defense: The Assessments and Recommendations of the National Defense Strategy Commission*. United States Institute of Peace (2018), pp 24-25.

OPERATIONAL CHALLENGE	TYPE OF INNOVATION		
	TECHNOLOGY	OP CONCEPTS	ORG / PROCESS
PROTECT BASES			
RAPIDLY REINFORCE / SUSTAIN			
INFO OPS / INFO ASSURANCE			
COUNTER A2/AD			
DETER /DEFEAT NUCLEAR/ WMD			
ENHANCE SPACE			
ENHANCE JOINT C4ISR			

An integrated approach should also balance incremental steps with potential step leaps, a feature of earlier DoD efforts at innovation, including the Office of the Force Transformation established in 2001. The work of this office, led initially by Arthur Cebrowski, built in part on the ideas of economist Eric Breinhocker, whose concept of innovative strategy emphasized maintaining foundational core competencies, expanding these core competencies, and placing big bets to develop entirely new competencies.[7] A workshop participant offered a similar construct: improve our ability to extract innovation from current investments and activities; repurpose existing capabilities, concepts, and organization/process to address new innovation needs; and develop entirely new innovation solutions as needed. Another variant of this approach would adopt an investment strategy focused on (i) "quick victories" targeting "low hanging fruit" to make some initial gains and jumpstart an innovation process; (ii) many incremental steps to achieve larger, but still modest, gains; and (iii) a few big bets that carry greater risk but have the potential to be transformative or achieve game-changing advances.

Fourth, we need an innovation infrastructure that enables the development, testing, wargaming and experimentation of concepts and technologies. This was the principal function of Joint Forces Command (JFCOM), created in 1999 to lead the DOD's military transformation effort, and disbanded in 2011. In light of the NDS and in recognition of new challenges facing the joint force, it is no surprise that the Joint Staff plans to resurrect a force-development and concepts organization in Norfolk, VA, where JFCOM was once headquartered. More broadly, there is a question of how to organize the DOD to best support innovation. Recent emphasis has been on creating small, tailored organizations (such as the Strategic Capabilities Office, Defense Innovation Unit – Experimental) that essentially work around standard RDT&E and procurement

7 Interview with Arthur K.Cebrowski, Director, Office of Force Transformation, *Defense AT&L* (March-April 2004) pp. 2-9.

processes. Whether relatively small-scale efforts like these provide the basis for a more broad-based innovation enterprise is not clear. Some workshop participants believe this remains a useful, pragmatic approach, assuming these organizations can pivot from the "find-fix-finish" mindset of the counter-terrorism/counter-insurgency mission to something more appropriate to great power competition.

It is also unclear whether more fundamental reform to organization and process are realistic. There is constant exhortation to do this, most recently in the NDS, but little progress has been made since the basic roadmap for acquisition reform was outlined by the Packard Commission in 1986[8]. The core question, then, is whether an effective basis for innovation can be achieved through various forms of adaptation or requires true transformation.

Fifth, we need the right metrics and measures of success. While there are useful metrics for gauging general progress toward broad innovation goals, such as investment budgets, number of patents and products, etc., it is also necessary to develop more dynamic operational and strategic metrics that are meaningful for assessing qualitative advances in military capability and their impact on competition with other great powers. Such metrics should follow from the basic organizing principles for innovation; if we organize (as suggested above) around a series of specific challenges framed by adversary advances that must be overcome to ensure operational success, then it should be possible to derive discrete measures of effectiveness relevant to assessing balances of power and our ability to keep adversaries at a disadvantage.

Sixth, we need to think more clearly about the role of culture in innovation strategy. Is culture an important factor in the ability of major powers to innovate effectively? If so, what aspects of national political, military, or scientific culture might be unique enablers of—or impediments to —innovation? Some hold to an assumption that the United States, with a culture characterized by a dynamic free market, an open political system, historically progressive immigration policies, and empowered soldiers, is inherently more competitive in any long-term contest in defense innovation. Regimes with largely state-centric economies may have an advantage in organizing and mobilizing resources with efficiency and discipline, but the imperative for political and social control will prove to be a substantial brake on innovation in technology and the armed forces. Others view this assumption as an example of cultural vanity that is dangerous as a basis for U.S. policy. More work is needed to understand the role of culture at this level.

At another level, there are questions about the need for cultural convergence between the DOD and the private sector firms critical to innovation. Widely reported accounts of employees at leading technology companies organizing resistance to doing business with the DOD in leading-edge security-relevant technologies such as

8 President's Blue Ribbon Commission on Defense Management, David Packard (Chairman). *Quest for Excellence. Final Report to the President*. https://www.documentcloud.org/documents/2695411-Packard-Commission. html (Accessed June 19, 2019).

artificial intelligence have fed the idea that there is a major cultural gap between the Pentagon and Silicon Valley, one that could become a significant obstacle to innovation. When pressed on this question, workshop participants from the private sector or who manage public-private initiatives have argued that this has been overblown. There are some high-profile examples, but overall the technology sector—which is composed largely of small firms—has few concerns about working on national security problems and indeed welcomes and seeks out this kind of work. If there is a gap, these speakers suggested, it is an experience, knowledge, vocabulary, and business-process gap, not a philosophical one—and therefore relatively easy to bridge.

Finally, we need to consider the ethical aspects of innovation. It is clear that some aspects of technological innovation raise serious normative questions when applied in the military sphere. This is not a trivial issue. The fact that the DOD has published ethical guidelines for the application of artificial intelligence confirms that this is important; so do the humanitarian campaigns being waged in Europe against innovations like "killer bots" and related efforts directed at autonomous systems. One question is whether ethical concerns are best addressed through a general framework or a more case-by-case approach. Another is how to address the likelihood that regimes that are authoritarian or face severe security dilemmas will not adhere to internationally adopted ethics-based constraints.

In sum, to out-innovate strategic competitors, there is a great deal that must come together effectively. We need

- realistic, strategy-driven, measurable goals;
- a sense of urgency and the means to accurately assess what others are doing;
- an integrated approach;
- an innovation infrastructure that enables the development, testing, wargaming, and experimentation of concepts and technologies;
- the right metrics and measures of success;
- a stronger understanding of the role of culture in enabling innovation; and
- a rigorous approach to consider the ethical aspects of innovation.

This is a broad and challenging agenda and requires sustained focus over a long period of time if the United States is to be successful.

Innovation and All-Domain Competition

Michael Markey

Does the strategy for S&T innovation address adequately all the military domains where major powers compete? As this question suggests, innovation must span all of the domains of military competition. Thus rating the efficacy of innovation strategy is not a simple matter. This short piece will present two frameworks for tackling the question of effectiveness.

The first framework we can use to clarify our thinking about innovation strategies is to divide conflict domains into the traditional and new. Generally speaking, the older traditional domains of conflict—land, sea, air, and nuclear—consume the largest percentage of defense spending, but newer domains—cyber and outer space—appear to be the largest targets of innovative thinking.

Innovation strategies for the traditional domains appear to be fairly responsive to the needs of the defense community and the warfighter. The responsiveness almost certainly stems from a consensus view shared by the Pentagon, the White House, and Congress on a U.S. defense strategy and acquisition plans to support the strategy. In other words, strategy drives innovation in traditional domains, and innovators can fill gaps identified by policymakers. Additionally, key stakeholders in the defense-contracting world almost certainly hold a shared vision of what the next evolutionary step in technology will be. Innovators can craft persuasive arguments to mature the emerging technology for the warfighter—whether it's faster aircraft, more precise missiles, or stealthier submarines—because the innovators intuitively appreciate the strategic needs of the U.S. and Washington's strategy in these domains. Furthermore, the traditional domains' predictable evolutionary innovation model allows university and contractor R&D departments to anticipate future DOD requirements and position themselves to reap profits while bolstering U.S. capabilities.

Unfortunately, this ecosystem is not operating well in regard to the newer domains of competition. Despite numerous DOD white papers and bureaucratic reorganizations, the U.S. policymaking community has not reached the same clear, strategic consensus on how to deter adversaries or wage war in the newer outer space and cyber domains. This lack of clear strategic direction translates into the absence of a clear innovation strategy directed at defense applications. This is not to say that innovation is lacking—commercial innovation continues to flourish as companies like SpaceX or FireEye field new products—but the drivers are lucrative profits and not the result of a collective governmental vision of military strategy and capability gaps.

Today, innovation is largely driving strategy formation, as government actors scramble to reap these innovations and apply them to cyber and outer-space strategies. It is possible, however, to reverse this approach and establish a paradigm in which government strategy formation takes precedence and the contractor base begins to innovate in ways that support a well-founded and widely-communicated government strategy. But current intragovernmental debates about outer-space strategy—currently linked to the establishment of a space force—or the role of cyberweapons in deterrence and warfighting strategies probably will dissuade contractors and other innovation hubs from investing too much in R&D efforts that may not yield profitable future businesses.

Apart from the framework above—dividing traditional from newer domains where strategy and innovation interact—is another framework that looks at how a nation fields forces in a domain. Michael Horowitz has argued that if a defense innovation is capital-intensive then incumbent, established great powers are advantaged. In his book *The Diffusion of Military Power*,[9] he cites historical case studies of the adoption of dreadnought-style warships prior to World War I as advantaging established great powers. On the other hand, defense innovations that require organizational innovations and upheaval in doctrine and tactics would find these same states at a disadvantage. The great powers often have invested enormous treasure in established capabilities and must contend with entrenched bureaucracies built around existing capabilities.

If we apply this framework (with hubris and without appropriate caveats) to our domains, we see that innovation in the land, air, sea, and nuclear domains will probably continue to advantage the U.S. and its allies. For the foreseeable future, we can assess that the most likely innovations that increase combat power in these domains are likely to be capital intensive and we can probably absorb these costs better than our potential competitors.

The new domains, however, present some problems for the U.S. because the innovations necessary to dominate the cyber and outer-space domains will require bureaucratic and organizational changes. As previously discussed, the U.S. is already struggling mightily with the organizational changes necessary to build and project combat power in the outer-space and cyber domains. Additionally, although outer-space capabilities will be expensive to field, the same may not be the case for cyberweapons, allowing a great leveling of the competitive landscape.

9 Michael C. Horowitz. *The Diffusion of Military Power*. Cause and Consequences of International Politics. Princeton University Press, New Jersey (2010).

S&T Innovation for National Security: a DOE Perspective

Madelyn Creedon

In thinking about defense innovation, the policy focus usually and naturally falls on the Department of Defense. But it is not the only source of innovation in and for the U.S. government. The Department of Energy (DOE) also plays an important role. From its inception in 1947, the Atomic Energy Commission (AEC), the successor to the Manhattan Project, was a research-and-development (R&D)-focused organization. While the nature of the research has shifted since that time, the DOE, as the organizational inheritor of the AEC mission, remains a preeminent R&D organization. Even the name—Department of Energy—is probably a misnomer. A more appropriate name would have been the Department of Science and Energy. In fiscal year 2019, DOE received $17.8 billion for R&D in a total budget of $35.5 billion. This short essay reviews the evolution of this role from 1947 to today and examines the sources of DOE's long-term success as a source of S&T excellence.

Atomic Energy Commission, 1947–1974

With the end of World War II, which led to the creation and use of the atomic bomb, U.S. policymakers became embroiled in a debate about the proper and necessary oversight of the continuing peaceful enterprise. Following an extensive congressional debate about the wisdom of having civilian control over the nuclear weapons establishment created by the Manhattan Project, the AEC was established in 1947. It inherited the vast decentralized Manhattan Project organization and structure. During World War II, the Army managers of the Manhattan Project, in their rush to develop a nuclear weapon, had turned to private industry to build, staff, and run, the vast complex scattered across the United States. There were few federal employees and thousands of contractors.

In establishing its own headquarters and structure, the first AEC chairman, David Lilienthal, a firm believer in decentralization, retained the Manhattan Project structure and the role of contractors in running the labs and facilities. The new Commission also inherited a complex that had been hastily built and not optimized for long-term research and production. One of the first tasks facing the AEC was rebuilding the physical infrastructure.

After the war ended, there was a general atrophy and loss of focus in the weapons complex as many of the top scientists returned to their home institutions. The long-lasting debate that eventually led to the decision to place atomic energy in civilian control also took a toll on the complex and contributed to a drift in the Army's interest in the project. Without the imperative to win the war, there was tension between weapons and materials production on the one hand and R&D into the promise of atomic energy for peaceful purposes—such as power reactors, basic atomic sciences, and the use of isotopes for a variety of purposes, including cancer research. Most outside of the Department of Defense, including many early AEC commissioners, recognized the growing demand for research on peaceful applications of nuclear energy and thought the AEC should focus on these uses.

The AEC advisory committee, led by Robert Oppenheimer, had a similar view and wielded a heavy hand in the early decisions of the AEC to move toward peaceful uses of nuclear energy. This committee pushed hard to evolve the AEC as a supporter of open research on basic nuclear sciences.

These new efforts were short lived, however, and weapons and materials won out following the first Soviet test of a nuclear weapon in 1949. The work of the AEC returned to producing weapons, usable fissionable materials, and nuclear weapons. Basic sciences, reactors, and the biological and environmental sciences remained important, but were not the priority.

The Air Force and Navy were also interested in new military applications of nuclear energy beyond nuclear weapons. This broader interest was important to the AEC and, as a result, the early foundations for the work-for-others program, now known as the Strategic Partnership Program (SPP), were laid when the Navy sent a small team to Oak Ridge to look at the possibility of nuclear reactors for ships. Captain Rickover was the lead for the Navy team. His year at Oak Ridge led Rickover to convince the Navy that nuclear propulsion was possible. A partnership was born and the AEC's new laboratory at Schenectady, New York, and the Idaho laboratory began to work on a reactor for the Navy.

The newly created Air Force started to look at reactors to power aircraft. Recognizing that long-range airpower was the future of warfare, the power provided by nuclear reactors was seen as an option to support high-speed, long-range bombers.

Energy Research and Development Administration, 1974–1977

The AEC continued until 1974, when Congress split the Commission into two new organizations, the Nuclear Regulatory Commission (NRC) and the Energy Research and Development Administration (ERDA). While the NRC was established to focus exclusively on civilian applications of nuclear energy, including the regulation of commercial nuclear power plants, the ERDA was Congress's effort to deal with the energy crisis of the early 1970s. Long gas lines, the result of a nationwide gasoline shortage, spurred Congress to establish the ERDA to focus on energy-related R&D and conservation initiatives. In addition to the nonregulatory mission of the AEC, the ERDA took on the tasks of the Federal Non-Nuclear Energy R&D Act and existing energy R&D programs from the Department of the Interior, the National Science Foundation, and other federal agencies.

Nuclear weapons and materials production remained a major part of the ERDA mission, but there was general concern that the new energy focus would distract from the national-security mission. Instead of taking on the old debate about civilian or military control of nuclear weapons, the statute creating the ERDA, the Energy Reorganization act of 1974, directed a joint study with the Secretary of Defense and ERDA administrator to see whether military applications of nuclear energy, the weapons side of the ERDA, should ultimately be transferred to the Department of Defense or another federal agency.

In the end, the study recommended the weapons mission stay at ERDA, but that visibility of the costs for nuclear weapons be increased and that there be a clear separation between management of the weapons programs and the energy programs. Secretary of Defense Rumsfeld was concerned that "top management attention to the expanding energy program may lead to erosion of weapons priority and funding in the future."[10]

From a congressional perspective, the powerful Joint Committee on Atomic Energy, which had overseen the AEC, was abolished. Oversight for military applications of nuclear energy—nuclear weapons and related work—was assigned to the Armed Services Committees, while responsibility for appropriations was moved to the energy and water subcommittees of the appropriations committees. This split, and the involvement of the Armed Services Committee, set up the very tension between civilian and military research and funding that Rumsfeld was worried about.

Department of Energy, 1977–Present

The energy crisis persisted, and Congress determined that the ERDA wasn't enough; a cabinet-level agency was needed to resolve the growing crisis. As a result, the Department of Energy was created by the Department of Energy Organization Act of 1977. Although the ERDA was established to deal with the energy crisis, a significant portion of the DOE funding was still dedicated to basic science research, thus leading to decades of confusion about DOE's work.

To emphasize the energy focus of the department, the DOE Act established an undersecretary with specific responsibility for energy conservation. The DOE's eleven statutory missions were split among eight assistant secretaries. More energy R&D and conservation functions from other agencies transferred in: the power administrations from DOI; responsibility for energy building standards from Housing and Urban Development; fuel-economy standards from the Department of Transportation; regulatory authority for oil pipelines from the Interstate Commerce Commission; and the Naval Petroleum Reserves from the Department of the Navy. The DOE Act also moved the Office of Naval Reactors to the assistant secretary for civilian nuclear energy, outside the weapons program.

10 *Funding and Management Alternatives for the Energy Research and Development Administration Military Applications and Restricted Data Functions*; report required by section 307(b) Pub. Law. No. 93-439.

The heavy focus on R&D remained, as did the organizational structure necessary for successful research and development. This included the laboratory and field-office structure, the patent, copyright, and licensing authorities, and no-year money. Having money that doesn't expire at the end of a fiscal year, unlike the constraints of most federal agencies, is one of the most important elements of funding multi-year R&D programs.

The DOE Act also specifically allowed military personnel to be assigned to DOE. Placing military personnel within the DOE helped to ensure coordination and visibility with DOD and the priority of the work on military applications, thus addressing Secretary Rumsfeld's concerns. Recognizing the importance of close coordination with DOD and in response to the earlier ERDA report, Congress made clear that military personnel assigned to DOE do not count against DOD military end-strength ceilings.

National Nuclear Security Administration, 1999–Present

Concerned that the focus on nuclear weapons and related activities was being eclipsed by the energy and science missions of the DOE, Congress established in 1999 the National Nuclear Security Administration (NNSA) as a semiautonomous entity within the DOE. The National Defense Authorization Act for Fiscal Year 1999 consolidated the nuclear weapons, naval reactors, emergency response, and nonproliferation missions of the department under a single administrator, who is dual-hatted as the undersecretary of energy for nuclear security.

The DOE's non-defense science, nuclear, and fossil-energy R&D activities were subsequently placed under an undersecretary of science. A direct report to the under secretary, the Office of Science continues the fundamental nuclear sciences from the AEC days, including basic energy science, biological and environmental research, fusion energy science, high-energy physics, and nuclear physics. This work remains driven by consensus science, with a long-term approach to advance basic science using world-class user facilities at the national laboratories.

The Advanced Research Projects Agency-Energy (ARPA-E), a congressionally-directed energy research entity patterned after DOD's Advanced Research Projects Agency (DARPA), reports directly to the Secretary of Energy and focuses on higher-risk energy-related research.

Like the rest of DOE, NNSA has a broad R&D mission. NNSA's national security focus is on weapons, nonproliferation, naval reactors, nuclear-materials transportation, and emergency-response missions. Ensuring that the quality of science remains high at NNSA laboratories and facilities is a top priority of the NNSA. Thanks to the authorities of the Atomic Energy Act of 1947, which were carried forward into subsequent legislation, NNSA has a broad variety of tools available to ensure world-class science. These tools include the participation of small businesses and universities using funds specifically set aside for work with university consortia and historically black colleges and universities (HBCU). NNSA continues to have the advantage of no-year money, the Strategic Partnership Program (SPP) and, most importantly the ability to use discretionary funds for laboratory and facility-directed research, in addition to significant mission-related research funding.

Keys to Research and Development Success

There are six structural reasons that DOE/NNSA has been a successful R&D agency.

1. Government-owned, contractor-operated (GOCO) facilities allow the private sector to bring expertise to managing the mission and science.
2. Most DOE laboratories and facilities have been designated as federally-funded R&D centers (FFRDC), which allow the DOE and other federal agencies to assign work that the government or commercial entities cannot perform.
3. The ability to do work for other federal agencies through the SPP expands the scope of work to a variety of challenging missions.
4. DOE can enter into cooperative R&D agreements (CRADAs) with any private entity so long as the DOE portion of the agreement does not exceed 50% of the cost.
5. DOE maintains maximum flexibility with no-year money that is available until expended, avoiding the end-of year rush to spend often experienced by other federal entities.
6. Laboratory-directed research and development (LDRD) provides the DOE labs and NNSA facilities with the opportunity to design and conduct their own research.

GOCO—The government-owned, contractor-operated structure, inherited from the AEC and implemented by management and operating (M&O) contractors, is unique to the DOE. Each the DOE facility, including all but one of the laboratories, is managed by one or more private M&O entities. The M&Os are generally single-purpose corporate entities established to manage a specific DOE facility or operation on a DOE facility. The corporate entity can be either a for-profit or not-for-profit entity. In the case of the NNSA laboratories and plants, all but one of the operating contracts is a for-profit entity. Historically, the AEC M&Os received minimal fees or were nonprofits managed by universities. Universities still play a considerable role in the management of the DOE facilities; the University of California is the predominate university partner in NNSA M&O contracts.

Though the operating contracts are generally for ten years—five years plus an option for an additional five—many M&Os have been in place much longer. The DOE and NNSA assess the M&O's performance on an annual basis to determine the fee that each M&O will be awarded and whether the contract will be extended. Each M&O has a unique fee structure set out in the contract and is allocated between fixed and award fees. Occasionally DOE or NNSA will choose not to renew or extend an M&O contract and will conduct a competition for a M&O contractor.

The M&Os provide market-based competitive salaries to attract top management talent and have a more flexible approach to contracting than the federal government. Generally, only the M&O leadership team changes when a new contract is put in place. Most of the actual workforce at DOE and NNSA facilities remain in place when an M&O changes, becoming employees of the successor M&O and thus ensuring program continuity and ongoing expertise.

This M&O system has generally served DOE well, although periodically the laboratories will argue that the inherent flexibility is being stifled by both Congress and the DOE. On the other hand, the balance between oversight and flexibility must be carefully managed to ensure best value for the taxpayer. As a result of these two competing schools of thought, there is often tension between the government and M&O. The mark of a good M&O is the ability to manage the tension constructively while meeting or exceeding the performance goals set out in the contract.

FFRDC and SPP—Most DOE laboratories and facilities are FFRDCs. At NNSA, the exception is the Naval reactor facilities, which are not FFRDCs. The FFRDC structure is not unique to DOE; other federal agencies, including the Department of Defense, use this flexible structure. One of the most advantageous characteristics of an FFRDC is that it can receive direct funding from a sponsoring agency as well as other federal agencies.

DOE refers to the projects that are directly funded by other federal agencies as strategic partnership projects. The SPP program, formerly known as the work-for-others program, supports a diverse range of work for many DOE laboratories and facilities. In addition to many DOE missions, NNSA in particular supports DOD, the Department of Homeland Security, and the intelligence community. Of the NNSA labs, Sandia is the most active, with just under half its budget coming from SPP projects. Most are short or quick-turnaround projects with fairly narrow applications, although that is not always the case. SPP projects tend to have very specific, near-term needs. Most of the SPP work is applied research, which in the case of an engineering laboratory such as Sandia, is a key tool for retention and to keep engineers at the cutting edge of technology development. A good example of this focused type of work is that which Sandia conducts for Special Operations forces.

The NNSA laboratories have also worked on small radars and space, air, and land -based sensors to detect radiation, multispectral and infrared signatures, and other unique sensors and detectors. Occasionally, NNSA labs and facilities have worked with industry on initial design or manufacturability issues. While, like all FFRDCs, NNSA can't compete with industry, NNSA can assist or partner with industry when called upon by a federal agency.

Historically NNSA and SPP projects have come under criticism for "parking" money from other federal agencies and perceived competition with industry. NNSA, however, carefully reviews these projects to conform to both law and regulation.

No-year money—Going back to history and the AEC, Congress determined that, given the nature of the work, the annual appropriations available to the AEC, and continuing today to much of DOE, are "available until expended." In other words, unlike other federal agencies that have money available for fixed periods of time, much of DOE and almost all NNSA funding does not expire or return to the treasury at the end of a fiscal year or period of years. This flexibility, which is also important to ensure nuclear weapons and materials remain secure at all times, also allows longer term R&D projects. Consistent funding, which is more assured under no-year money, avoids the year-end rush to spend money and the associated criticism. That said, the rate at which funds are expended is monitored closely by Congress and the DOE budget office. If DOE or NNSA build up large prior-year balances, Congress can rescind those funds and direct that they be used for other purposes.

While the no-year money is a benefit to R&D, the DOE's approach to funding major construction projects, including science facilities, can be an issue. Money appropriated for a construction project is also no-year money, but the DOE and NNSA receive the construction funding on an annual incremental basis designated by project, unlike the DOD, which gets most of its major construction money up front. While there are exceptions for some major projects, such as hospitals, DOD construction projects are less subject to the disruption annual funding can cause.

Project schedules are often shaped by available funding, which can cause the scope to be modified or spending stretched out over many years. As a result, the costs of a project can increase or the final project may not meet original expectations. This funding approach is very challenging, as most NNSA and DOE Office of Science facilities are first-of-a-kind, one-of-a-kind-facilities, with finding spread out over many years.

There is one additional aspect of construction funding that presents a significant problem for NNSA laboratories and SPP work. This funding is generally provided by the sponsoring agency on a time-and-materials basis. While the NNSA entity is able to use the funding to purchase small items of equipment, it may not use the funds for construction projects.

Other agencies are reluctant to fund construction projects on DOE sites and NNSA is reluctant to use its scarce resources to fund a multipurpose project. Lawrence Livermore National Laboratory has tried to get at this problem through third-party financing, but has been unsuccessful so far. Sandia was able to use some discretionary minor-construction funding to refurbish an existing older building that is now used for multiple SPP projects, but has also struggled to address this problem. To ensure long-term scientific and engineering expertise in the nuclear security complex, NNSA will have to resolve the funding dilemma for new multipurpose buildings and facilities. While NNSA has taken some initial steps to focus on the overall health of the laboratories and facilities, not just the facilities that sustain the NNSA mission, success will require the support of Congress and the Office of Management and Budget.

CRADAs—Another important tool that DOE and NNSA laboratories and facilities use to partner with private industry are cooperative research-and-development agreements (CRADAs). No more than 50% of the cost of the project covered by a CRADA may be funded by a laboratory or facility, but either party can use in-kind contributions to meet their respective commitments. CRADAs are not unique to DOE, but provide some creative and interesting uses of core capabilities, an opportunity work with industry, opportunities for laboratory personal to do something different, and incentive for retention.

LDRD/PDRD—Laboratory- and plant-directed research and development (LDRD) is one of the most important tools in the DOE and NNSA research toolkit. LDRD provides R&D that underpins much of the innovation for the NNSA missions and provides considerable freedom for laboratories and facilities to do creative cutting-edge research. Although LDRD was an important part of the R&D effort in prior years, specific statutory authority for LDRD was provided in the 1991 National Defense Authorization Act (NDAA) for all Atomic Energy Defense -funded laboratories—the three NNSA national labs and the NR labs. The specific purpose of LDRD as set out in the statute is to:

- maintain the scientific and technical vitality of the laboratories;
- enhance the laboratories' ability to address current and future DOE/NNSA missions;
- foster creativity and stimulate exploration of forefront areas of science and technology;
- serve as a proving ground for new concepts in research and development; and
- support high-risk, potentially high-value research and development.

LDRD funds, however, must **not** be used to:

- substitute for or increase funding for any tasks for which a specific limitation has been established by Congress or the Department or for any specific tasks that are funded by DOE/NNSA or other users of the laboratory;
- fund projects that will require the addition of non-LDRD funds to accomplish the technical goals of the LDRD project, except as provided by legislation;
- fund construction design beyond the preliminary phase (e.g., conceptual design, Title I design work, or any similar or more advanced design effort) or fund line-item construction projects, in whole or in part; or
- fund general purpose capital expenditures with the exception of acquisition of general-purpose equipment that is clearly required for the project and is not otherwise readily available from laboratory inventory.

Plant-directed research and development (PDRD), which also included the Nevada Test Site (now the Nevada National Security Site), is subject to lower limits than LDRD. SDRD and PDRD are 4% of the facility budget and project costs, while LDRD is 6%. The LDRD percentage was raised to 8% in the 2006 Consolidated Appropriations Act, which also expanded LDRD to all DOE national labs. The LDRD percentage was later reduced to 6% in the 2014 Energy and Water Appropriations Act.

LDRD/PDRD funding, which is in essence a tax on all laboratory and plant work, is a substantial investment. Per the LDRD report for fiscal year 2018, NNSA generated $13 billion, of which $10.9 billion was from DOE/NNSA sources, $2.6B from SPP projects for LDRD, and $3 billion for PDRD at the NNSA sites. The five largest DOE-wide beneficiaries of LDRD funding are Sandia National Laboratories at $3B; Los Alamos National Laboratory at $2.1B; Lawrence Livermore National Laboratory at $1.6B; Oak Ridge National Laboratory at $1.2B; and Idaho National Laboratory at $1B.

Congress has been generally supportive of LDRD, but the program has its detractors. Over the years, the initial statutory authority was amended to ensure that LDRD and PDRD work derived from DOE mission funding was relevant to the DOE mission and work using funding derived from SPP projects was relevant to the work of the sponsoring agency.

LDRD and PDRD funding is a highly competitive process with only about 25% of the submitted proposals selected. The NNSA laboratories and facilities put out guidance, which is approved by NNSA. NNSA also approves each project selected but does so with a light touch, mostly to ensure that the projects don't violate the regulations and statutory authority. As a general rule, NNSA does pass judgment on the science of the proposed projects unless requested by the laboratory or facility. NNSA and the laboratories and facilities share a common interest in ensuring that the projects fit the missions.

Judging Success

All of the tools, although excellent, do not ensure high-quality science. Thus, a recurring question is how do DOE and NNSA judge success? This a difficult question to answer and one that the National Academy of Science examined extensively over the course of about nine years in two reports.[11],[12] Ultimately one of the recommendations from the reports was that Congress and NNSA maintain strong support for the LDRD program, as it is an essential component of enabling the long-term viability of the laboratories. Other indicators of success include the number of R&D 100 awards that the DOE laboratories win. For the past 30

11 National Research Council. *Managing for High-Quality Science and Engineering at the NNSA National Security Laboratories*. The National Academies Press, Washington DC. https://doi.org/10.17226/11009 (2013).

12 National Research Council. *Maintaining High Scientific Quality at Los Alamos National Laboratory and Lawrence Livermore National Laboratory*. The National Academies Press. Washington DC. https://doi.org/10.17226/13367 (2004).

years, the DOE has won, on average, approximately 30 awards per year. From the beginning of the Manhattan Project, 115 Nobel laureates have been connected with the labs and plants.

Another strong indicator of success for the NNSA SPP program comes from the customers themselves. The NNSA labs are generally viewed by many other federal agencies as expensive and yet the quality of work keeps those sponsors returning to the NNSA facilities.

In spite of the tools and the history of scientific success, the future is uncertain. Competition for top scientists and engineers is fierce, budgets are always uncertain, and security clearances take too long to process. Congress, DOE, and NNSA will have to be vigilant to ensure the quality of science and engineering and other technical skills at the DOE and NNSA laboratories and facilities remains top notch and meet the requirements of many missions. NNSA must be a steward of the entire laboratory or facility, not just those portions that carry out NNSA work, to ensure long-term viability and technical excellence. Without focus, attention, and commitment from both the executive and legislative branches of government, the next 70 years might not be as successful.

From Innovation to Capability: Lessons from the Past

Michael May

Innovation is newly prominent in U.S. defense strategy, but it is hardly new. Science and technology (S&T) competition played a major role in the prosecution of World War II and through the Cold War, and the United States and its allies won in part because of their superior capacities for innovation. Such competition became much less prominent in U.S. strategy in the period after the demise of the Soviet Union, even as it became more prominent in the strategies of China and Russia, among others. Top-flight competition is stiffer now than before, and in key areas the United States no longer leads. Moreover, we face an expanding set of innovation challenges, arising not just from major power rivals but also from the emergence of new global challenges associated with, for example, climate change. Powerful as we are, the United states is only 330 million people out of several billion globally—and the billions are growing faster than we are. We must again up our innovation game, so to speak. We must not only innovate but out-innovate our strategic competitors and our new strategic challenges. It is more important than ever that we "get innovation right." What does this require? Our past success offers some useful guideposts for the future.

This contribution is divided into three parts. First, I will briefly review the ingredients needed to encourage and nurture innovation. Next, I will note the obstacles to implementing those steps, obstacles that have also long been identified but have proven difficult to change. Finally, I will give a personal view on what's needed to bring back a level of defense innovation adequate to the coming times.

The Environment for Innovation

There are many dos and don'ts in this area. I limit myself to three ingredients for a successful environment for innovation.

1. ***Posing the right question*** is essential if innovation is to lead to new useful capability. When the U.S. Air Force sponsored the project that would become the RAND Corporation, General Hap Arnold, then USAF chief of staff told the project heads, "I want you to tell me what questions to ask you." The right question can come from questioning the state-of-the-art of a technology or science, from recognizing an existing vulnerability or an overlooked opportunity, from thinking about a new mission or taking a new look at an old one, or often from a combination of these. It can be posed by an investigator or by one of the leaders or even from the customer—in our case, Washington. But it must be broad enough to allow the investigator

to step back from a problem and look for alternatives to present ways of thinking and doing. Stove-piping R&D areas is an enemy of innovation.

2. ***There must be sufficient time and resources to make and correct mistakes.*** Even the best ideas involve trial and error. The people doing the innovating must be trusted enough to allow for those. This means that enough time must be available. At some point of development, trial and error must stop and a schedule must be established and adhered to. Where that point is depends on many variables and establishing it requires informed technical and managerial leadership. But attempting to pace the investigation by means of milestones and progress reports before that point is reached is also the enemy of innovation.

3. ***An informed "buyer" and a short chain of approval are valuable.*** A knowledgeable "buyer" in the relevant government agency, committed to the common goal, is far more valuable in fostering innovation than one who does not understand the issues involved in the field, cannot grasp the goal or the ways to it, and can only measure performance by adherence to schedules and regulations. Those are necessary to complete large projects but should not be applied to organizations where new ideas are generated.

A foreword that David Packard wrote to the report of the Blue Ribbon Commission on Defense Management, which he chaired in 1986 at the request of President Reagan, remains relevant:

> *Excellence in defense management cannot and will not emerge by legislation and directive. Excellence requires the opposite – responsibility and authority placed firmly in the hands of those at the working level, which have knowledge and enthusiasm for the tasks at hand. To accomplish this, ways must be found to restore a sense of shared purpose and mutual confidence among Congress, DOD and industry. Each must forsake its current ways of doing business in favor of a renewed quest for excellence.*[13]

Several different administrative structures can provide an environment favorable to innovation. At Lawrence Livermore National Laboratory, important innovations were made within the nuclear weapons program and the National Ignition Facility (NIF) program. They were also made in laboratory-directed research and development (LDRD) programs that are not coupled so tightly to a large effort. Modern satellites

---

13 *A Quest for Excellence* Final Report to the President by the President's Blue Ribbon Commission on Defense Management June 1986, page xi, Foreword by David Packard https://www.documentcloud.org/documents/2695411-Packard-Commission.html (Accessed September 4, 2019)

and modern stealth aircraft stemmed from earlier smaller innovative efforts by air- and space contractors. Today, the knowledge, the people, the structures are in place. Nevertheless, defense program innovation is lagging behind the pace and breadth needed. The problems seem to be mainly, not in generating ideas,[14] but in moving ideas into the needed systems.

During the Cold War, the U.S., imperfect as it was, had a definite edge over the Soviet Union. I remember discussing this with a very productive Soviet scientist in the fusion program, whose ideas are now widely implemented. He relayed that to get the funds and permission to test some of his ideas, he had to go through his local director, through the relevant minister who then communicated his request to another minister, who sent the request to another firm, which then fulfilled it—but it was usually wrong because of the communication difficulties.

It is an open question whether the U.S. can maintain this edge against a very different opponent like China. The Chinese government is acutely aware that China is number two and must run harder. President Xi's very ambitious defense program provides a direction and a spur to innovative capabilities.[15] China, a huge country with a complex and imperfect governing structure, has its own problems, but has achieved major changes and is continuing to change. It is also far more open to the world, scientifically, technologically, and commercially than the Soviet Union was. These are major advantages given that today, unlike the situation after World War II, excellent R&D relevant to defense programs exists in many parts of the world.

The Obstacles to Innovation

The obstacles to innovation in defense programs stem mainly from the costs, time delays, and overregulation imposed by our own system on the implementation of new projects. Speakers at this workshop have detailed how current obstacles have affected the pace of innovation and the ease with which they can lead to new capabilities. Some problems are new, but most are not. Again, Packard wrote,

> *DOD must displace systems that measure quality by regulatory compliance and solve problems by executive fiat. Excellence in defense management cannot be achieved by the numerous management layers, large staffs and countless regulations in place today. It depends, as the Commission has observed by adhering closely to basic, common-sense principles: giving a few capable people the authority and responsibility to do their job, maintaining short lines of communication, holding people accountable for results.*

14 See, for instance, *The Future Postponed*, April 2015, Cambridge, Massachusetts. https://dc.mit.edu/sites/default/files/Future Postponed.pdf (Accessed August 15, 2019).

15 John W. Lewis & Xue Litai. *China's Security Agenda Transcends the South China Sea*, Bulletin of the Atomic Scientists, 72:4;pp 212-221, DOI: 10.1080/00963402.2016.1194056 (2016).

Several studies have been undertaken that look at what has happened in the thirty-some years since Packard submitted his report. One was the 2015 effort at rethinking the Packard Commission report by Jacques Gansler, former undersecretary of defense for acquisition, technology and logistics, based on a CSIS study.[16] Its conclusion, and that of others, is that while a number of reforms were implemented and did help, by and large the problems identified in the commission report remain.

Some of this may be inherent in the size of the U.S. establishment and some to the complexity of modern systems. But comparing the speed with which innovation led to important, crucial new defense capabilities in the early Cold War era to the present day points to something else that is missing: the existence of what were new missions at the time, such as stable deterrence, timely worldwide intelligence, and alliance support. All these missions were judged to be crucial to the survival of the United States, as well as new. Threats to survival have two beneficial results: they focus the mind on getting things done whatever the system flaws and they show where innovation is most needed. But these results are achieved only if they are recognized and guiding policies and strategies are developed.

It is recognized that stable nuclear and non-nuclear deterrence, timely worldwide intelligence, and alliances remain as crucial to survival as ever they were, but they have lost their ability to mobilize the defense organizations sufficiently to break established and counterproductive patterns of development and procurement. The U.S. commercial sector continues to innovate and to translate innovation into capability. Competition, where it exists, keeps it mobilized. The U.S. defense sector, particularly its development and acquisition arms, are not so mobilized, even though the old threats and needs are still there and several new threats exist. Have the threats been recognized? Has this led to formulating new missions?

The Unmet Need

Bringing up new threats immediately leads to the issue of terrorism—a threat that has been identified. An overall strategy exists which, by whatever name is preferred, amounts to a global war on terror. As a result, missions have been defined and needs identified, and there has been some innovation—for instance in war fighting against Al Qaeda and the Islamic State. A great deal remains to be done, in intelligence coordination and in the related area of cyber warfare, but the country has at least mobilized to meet that threat.

In two other areas, the U.S. faces new survival threats but guiding policies and strategies do not exist, thereby hampering or preventing defining new missions, identifying new needs and providing both motivation and guidance for innovation to play its role. First, the DOD, the military, and some in Congress have recognized

16 The Honorable Jacques S. Gansler. *Defense Acquisition Reform: Rethinking the Packard Commission Approach After 30 Years*, Center for Strategic and International Studies (July 17, 2015).

that global climate change threats need to be addressed. Some steps have been taken, such as safeguarding military bases and other assets, but these are marginal in meeting the main threats. These steps do not deal with consequences that have already been identified, such as shrinking of human habitats, widespread food shortages, and consequent unrest, political upheavals, and migrations. Many of the tools needed to deal with these problems lie outside the defense area of responsibility, but dealing with them will also generate new defense needs.

An adequate defense posture to deal with such eventualities can only exist in the context of an adequate national policy. Such a national policy will be difficult to arrive at under current circumstances. Global coordination and commitment are needed, as they were also after World War II. With the 2015 Paris Agreement, there was a start but progress has been stymied. Formulating a national policy is in abeyance, let alone international coordination, yet there may be a role for preliminary thinking aimed at identifying defense needs and possible missions to meet broader eventualities than the ones considered to date.

A second area where the U.S. may face a threat, if not to immediate survival at least to defense and intelligence capabilities, is the shifting sentiment toward alliances that has begun to take place. Alliances have been essential to U.S. security and its overall position in the world. They remain formally in place and fortunately they retain considerable political support. But the foundations have been shaken, in part by a pattern of recent U.S. statements, in part by the shifting balance of power in the world, and in part because a renewed case for alliances, based on current threats and opportunities, has not been made.

There is little talk about the possible effects on U.S. security and defense missions of weakened or shifting alliances—very likely because of the fear that overt discussions and planning could help precipitate the very decay of mutual trust essential to any lasting alliance. This may be appropriate, yet there are unmet defense needs if our alliances weaken and probably also unmet needs to shore-up those alliances. Again, if these needs are not identified, missions cannot be defined, and there is no clear goal for innovation.

Both of these threats—climate change and the weakening of alliances—are scary to think about. At the end of World War II, nuclear weapons were scary to think about, as were the devastated state of Europe and the threat posed by the Soviet Union. Out of those fears, a lasting policy was forged, which led in turn to new capabilities and considerable innovation. Fear coupled with adequate leadership create an atmosphere where, it is clear, not only innovation was needed, but also a timely and essential translation of technical advances into new systems. Together they have been and could again be a force against the factors that slow or prevent progress.

The two threats just discussed differ from the threats seen at the end of World War II, in that the post-World War II threats were widely seen as being imminent, while climate change and the weakening of alliances are happening in slow motion.

In addition, World War II mobilized the whole nation, and the resulting sixty million dead showed what could be at stake in global threats. It is more difficult now to rally the large popular support and large commitments needed, even though there is no less need.

Consensus can be built. In the case of climate change, the Paris Agreement showed that consensus on initial commitments to reduce greenhouse gas emissions could be built among 174 widely different countries. Much wider cooperation involving much more difficult decisions will eventually be needed, but a first step was taken. In the case of alliances, damage has been done, but there is enough support in the U.S. and abroad to rebuild consensus there also. In either threat area however, if we wait too long, reversing adverse trends would prove difficult and eventually impossible.

Closing Observations

In developing our thinking about how to "get innovation right," it is important to recognize that we are not starting from scratch. As a nation, we have decades of experience in competing and seeking to out-innovate competitors. Although that experience occurred in the unique circumstances of the past, it can nonetheless offer useful lessons about how to generate and sustain innovation in a manner that produces new capabilities for national security. In today's security environment, however, the needed new capabilities are not just in the military domain. With the emergence of a broader and broadening set of challenges, our innovation strategies must adapt further.

The Building Blocks of a Successful Innovation Strategy

Nerayo Teclemariam

As a relative newcomer to the nuclear enterprise, I cannot contribute an analysis of the lessons of the past for science and technology (S&T) innovation, except as I have learned them from others. So let me offer a perspective that reflects my experience as someone attracted to the labs a few years ago, partly because of the significant opportunities there to combine S&T leadership with public service. I will make three arguments about how to overcome obstacles to successful innovation. First, innovation is a means to an end and thus successful innovation requires clarity about objectives and metrics. Second, successful innovation requires an ecosystem encompassing not just practices and technologies, but also people and culture. Third, the key to success in the national security sector is to leverage strengths outside that sector—a key that has so far been elusive.

What is Success?

Innovation is a means to an end and not an end in itself. The only meaningful metric of success is whether the end is achieved. This puts a premium on having clarity about that end. Innovation must be guided by a purpose and that purpose is the sole metric of success. Too often a goal is set to innovate on a specific topic (e.g., artificial intelligence in the cyberspace) without communicating (or perhaps even understanding) the real-world operational problem that must be addressed. In the debate about defense innovation, the expert community tends to fall back on the "unmet operational challenges" outlined in the National Defense Strategy and discussed earlier in this volume. But we must ask whether they accurately capture the operational problems that need to be solved.

The same precision is needed when it comes to identifying the obstacles that must be overcome if an innovation strategy is to be successful. The description of the obstacle must be sufficiently precise to allow the solution providers to clearly understand the problem and at the same time not over-specify the desired solution. This breadth allows innovators to explore nontraditional solutions to problems. Innovations must ultimately result in fielded and deployed operational capabilities to be considered a success—although there can and should be lots of failures along the way. In order to gain the confidence of end-users of the innovation, the solution must be tested in relevant environments. This could potentially be done initially in synthetic environments to gain confidence early in the development cycle, but small-scale deployments in real environments are the ultimate test and validation for end users. Once the right operationally-relevant problem has been defined with a balance of specificity and breadth, innovation can be brought to bear and the resulting product tested for deployment.

Are There Metrics? Revisiting Scope

In considering metrics to track and manage innovation, we must again stop to define the scope of the innovation domain. Given the prevalence and focus on technology in various U.S. strategy documents and calls for proposals from U.S. government agencies, there is a strong emphasis on R&D to develop technological innovations. However, innovation in the entire R&D value delivery change needs to be considered, including processes, people, and organizational structures. Within each of these areas, separate metrics can be defined and measured. Based on personal past experience and discussion with current R&D researchers, it could be argued that technical innovation is by far the easiest part of a project, and securing funding, contracting, and working through organizational bureaucracy is the larger challenge and worthy of more innovation.

A typical metric for innovation is return on the investment (ROI), which involves quantifying the investments or inputs of the innovation process to include money, time, or talent devoted to a specific activity and the impact of the investment (e.g., knowledge generated and transferred). The innovation process can be simplified into a conceptual in-and-out flow model.

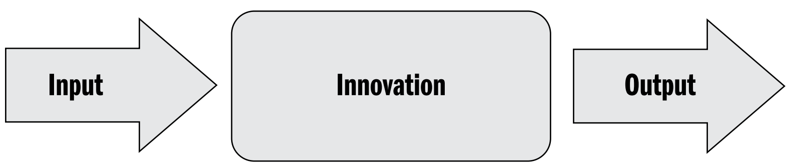

Figure 1. Innovation flow.

Some examples of input metrics include:

- R&D spent as a percentage of gross domestic product (GDP);
- number of innovation projects started in a given time period;
- number of new ideas in the pipeline at each technology readiness level; and
- number of new employees in R&D.

Some examples of output metrics include:

- number of transitioned/deployed innovations;
- patents filed and what fraction are licensed by corporations;
- ROI of innovation activities and system-wide cost savings; and
- number of staff trained or exposure to national security enterprise.

There is a need to take into account the entire innovation system when calculating the ROI, because there could be system-wide cost savings by deploying an innovation that eliminated unnecessary steps. Moreover, organizations need to constantly evaluate current innovations and filed patents and determine if they should be allowed to expire, as there is a monetary cost to maintain and renew them. Finally, it is a common desire for inventors to follow their creations to market via separation from their R&D labs and transition to the private sector. The brain drain from the R&D lab to the private sector has historically been seen as a negative metric by federal government R&D organizations; however, if supporting the full life-cycle of innovation is the overarching goal of U.S. policy, then allowing and supporting the flow of talent through the innovation life-cycle might lead to faster and effective deployment outside, and ultimately be considered a positive metric.

The DOE national laboratories have recently implemented entrepreneurial leave programs that allow researchers to take a leave of absence from their position to support the adoption of their creations in the private sector. The labs hold the researcher's laboratory position for a number of years and allow them to return if the venture in business transition fails. This job security reduces the risk for the innovator to provide support for bringing technology to market. Another metric to consider when evaluating the entire impact of an innovation is measuring the number of R&D professionals and student interns exposed to key innovation problems for defense application. This bolsters the pipeline of talent and ultimately grows the brain trust for the entire national innovation base.

What are the Barriers to More Effective Innovation?

Having considered what success is and the potential metrics, we now turn to the question of barriers to more effective innovation. The Defense Innovation Board is composed of members from the private sector and academia who offer a useful framework to consider the totality of the innovation ecosystem. Their recommendations[17] to improve innovation are captured in three general categories: (1) people and culture, (2) technologies and capabilities, and (3) practices and operations.

People and Culture Beginning with people and culture, we can break this category down into various subcultures, including the private sector, academia, and the national security industrial base. Considering the private sector and academic ethos, there exists a growing body of literature highlighting a disconnect between those communities and the U.S. government. Former secretary of defense Ash Carter recently argued that U.S. innovators in both the public and private sectors

17 Defense Innovation Board. https://innovation.defense.gov/Recommendations/ (Accessed April 15, 2019).

need to take the public purpose into account when they develop new technologies.[18] Furthermore, millennial civilians have been found to possess a great respect for military service, but do not want to serve or contribute.[19] As a borderline millennial, I would put forth that my generation is very much committed to global service and motivated with a desire to have an impact; however, we see that there are multiple pathways to achieve this—especially through the private sector. Studies have shown that millennials view the issue of climate change as more pressing than current national security and defense challenges.[20] As has been noted in U.S. Department of Defense (DOD) publications, the two issues are intertwined, but this realization is not well known or communicated to millennials, the private sector, or academia.[21] In my personal experience during frequent recruiting trips on college campuses, many students talk about (and demonstrate) that they want to have an impact. The distrust and lack of understanding of the national security enterprise are high and there exists a need to change the narrative, or the national security community will be unable to effectively partner with a valuable source of talent.

Regarding the culture of the national security industrial base, it has long been noted that institutional bureaucracy is an innovation killer. Focus has been placed on formalizing processes to manage cost and risk rather than on promoting innovation and speed. This has resulted in long innovation- and requirements-generation times involving coordination between multiple stakeholders. Furthermore, risk tolerance is low for mission work, which challenges both the speed and need for innovation. This has not always been the case when examining the history of defense innovations. For example, the innovation of new nuclear weapon designs in the late 1940s was remarkably fast and yielded multiple, fielded systems on timescales much faster than today. That environment is very similar to the speed of cybersecurity innovations that we are currently seeing around the world.

I would like to note that an extensive amount of innovation does occur in the national security industrial base that supports basic R&D, including that at the DOE national laboratories via their LDRD programs.[22] These funds have been established to promote innovation in basic and applied R&D that is high-risk and potentially high-value. The stigma researchers experience for failure is low in this program, because of an explicit focus on exploration, which promotes a culture of innovation and risk taking.

18 Ash Carter. *America Needs to Align Technology With a Public Purpose*. The Atlantic. (November 25, 2018) https://www.theatlantic.com/ideas/archive/2018/11/mark-zuckerbergmissed-opportunity/576088/ (Accessed August 15, 2019).

19 Ender M.G., Rohall D.E., Matthews M.D. *Millennials' Attitudes toward Military Service. In: The Millennial Generation and National Defense: Attitudes of Future Military and Civilian Leaders*. Palgrave Pivot, London (2014).

20 https://www.weforum.org/agenda/2018/01/this-is-what-millennials-want-in-2018/ (Accessed April 15, 2019).

21 U.S. Department of Defense. Report on Effects of a Changing Climate to the Department of Defense. (RefID:9-D30BE5A) (2019). https://media.defense.gov/2019/Jan/29/2002084200/-1/-1/1/CLIMATE-CHANGE-REPORT-2019.PDF (Accessed August 15, 2019).

22 https://www.energy.gov/cfo/listings/laboratory-directed-research-and-development-annual-reports (Accessed April 15, 2019).

The end-user community, another culture to consider, includes those who will have to use the technology or processes created by innovation. Unfortunately, these communities are largely left out in the full innovation cycle. Their feedback is typically captured in the front end of the innovation process, via requirements, and they are then expected to field and use the innovation when development is complete. However, it is not uncommon to see limited testing and training budgets devoted to support deployments, which results in unprepared end users and failed technology transfer. This disconnect in support of the fielding and deployment of innovations causes technologies to be shelved as too difficult to field. When end-user needs are re-identified the following year, the same innovation process results in the reinvention of previous technologies, followed by a repeated transition failure.

Practices and Operations Turning to innovation practices, there are two popular and competing views regarding idea generation and solution finding in various communities. The first process, which we will call "requirements driven," is centered on asking the end user what he wants from a future innovation, and then distilling that feedback to a set of requirements that drive the innovation space. This process works well for capturing incremental advances of technologies and where the concept of operations (CONOPs) is well understood. The second and competing process for innovating is centered around "design thinking"[23] or the "customer discovery process."[24] These approaches, championed by famed private-sector companies like IDEO and Apple, entrepreneurs like Steve Blank, and institutions like Stanford University's design school have grown in acceptance and are staples in innovation hubs like Silicon Valley. This innovation model is centered on the innovator observing the end-user's workflow and exploring pain points through a structured elicitation process and feedback on rapidly-developed prototypes. A powerful underlying assumption with this approach is that the end-user cannot even envision the future in which he could live or how CONOPs could be radically altered. It is the innovator's job to extract the true need of the end user and what is valued, not what the end user said was wanted. This innovative approach can be highly disruptive and change the course of entire sectors when successful. As an example, around 2007, if a cell-phone innovator asked end users what characteristics they would want in a phone, they would have likely expressed a desire for a slimmer, lighter flip phone like the Motorola Razr. End users had no concept at that time of an Apple iPhone or the radical changes that it would bring, such as an app store with third-party developers and an interface with only one physical button. This type of innovation is challenging to replicate in a formal requirements-driven approach and requires a "customer discovery process" a complete change of the concept of operations.

23 https://dschool.stanford.edu/resources-collections/a-virtual-crash-course-in-design-thinking (Accessed April 15, 2019).

24 https://www.slideshare.net/sblank/customer-discovery-23251533 (Accessed April 15, 2019).

What Can be Done to Address the Barriers?

Although the barriers to innovation can be challenging, there are a number of approaches that can be taken by the U.S. government to address and mitigate them. The technical research and development pipeline can be broken down to three distinct stages: basic research, applied research, and development. Data from the National Science Foundation[25] continues to show that federal R&D dominates at the basic-research level, where the failure risk of ideas is highest, and industry plays a smaller role. Federal R&D also provides a significant fraction of funding to applied R&D where funding levels are roughly split with industry. In the development phase of the pipeline, the data show that industry investment dominates and there is likely little influence that federal spending can rival current levels.

Basic Research In order to maximize their investment, the U.S. federal government should focus on the basic and applied research stages where investment levels could have the highest return on investment. There are examples in the current federal government where this approach has been recognized and aligned to. For example, the DOE LDRD portfolio emphasizes "discovery class" basic and applied science that promotes high-risk, high-value exploration of innovations. Failing forward and failing fast are seen as advantageous rather than hurtful to innovation. There are also a number of public–private consortium business models that enable the leveraging of investments from multiple parties. For example, the DOE Energy Efficiency and Renewable Energy (EERE) and Vehicle Technology Office (VTO) foster consortiums of national laboratories, industry, and academic partners focused around specific R&D challenges. The consortium members (e.g., U.S. Drive[26]) agree on a research agenda that focuses on "pre-competitive" challenges, which allows the pooling of funding to tackle the largest, cross-cutting barriers. The agreement still enables industry to compete against each other during the later applied and development stages of innovation. These consortia require extensive coordination and agreement, but they can be powerful tools to leverage and multiply investments from various parties to accelerate technical progress from basic science to market.

Applied Research In the applied-research phase, where federal investment is on par with industry investments, the consortium model noted above can also have value. Moreover, the forty-two federally funded research and development centers (FFRDCs) and the national industrial base have demonstrated tremendous value and innovation when exploring problems at the interfaces of fields (e.g., autonomy for

25 https://www.nsf.gov/statistics/2018/nsb20181/?org=NSF (Accessed April 15, 2019).

26 https://www.energy.gov/eere/vehicles/us-drive (Accessed April 15, 2019).

hypersonics[27]), where there is typically a lack of attention because of organizational and funding silos. These are potentially key areas where innovation is lacking and the federal government, via FFRDCs, can offer outsize impact on the innovation landscape.

Development The development phase of innovation is largely dominated by industry funding. Federal funding in this phase will have minimal impact compared to industry, except in cases where support for niche, new industries are needed and venture capital or access to public markets for companies is lacking due to risk. For example, FFRDCs have supported the development of open technology standards to promote innovation in national security areas where market forces have traditionally supported a closed community of service providers. New vendors desire to compete in these markets but are locked out due to proprietary standards used by integrated service providers. By transitioning to open standards, new vendors can bring innovation to specific components without having to provide a fully integrated system. A recent success is the Transportation Security Agency and its Open Threat Architecture Platform (OTAP) program,[28] which is developing open standards for next-generation X-ray detection technologies to allow plug-and-play opportunities for new third-party vendors to provide detection algorithms. Competing industry vendors find value in working with FFRDCs because they pose no threat to vendor commercial interests and can adjudicate cross-vendor technical issues more objectively than other organizational alternatives. This open architecture has enabled other parts of government to access previously unavailable innovation. For example, the Department of Homeland Security Science and Technology Directorate funded the Google-owned company Kaggle to host an image-recognition detection competition with a prize pool of $1.5 million dollars.[29] Over 149 teams competed for the prize money, and the winning algorithms were transferred to the U.S. government, vetted by an FFRDC team, and loaded onto an X-ray system using the OTAP-designed open standards. The program still has much work to be done to be considered a success, but the innovation environment that it enables is very promising. Additional programs in other parts of the U.S. government seek to follow similar process.[30]

Staying on the topic of FFRDC innovations, there is a growing emphasis, as evident from the 2017 National Security Strategy and 2018 Nuclear Posture Review, on enhancing innovation for rapid development of solutions for national security. As noted above, the basic science and technology research funded within the nuclear weapons complex and the DOE FFRDCs (i.e., LDRD) has always been risk tolerant, but

27 http://www.nationaldefensemagazine.org/articles/2018/8/14/rd-special-report-federally-funded-research-labs (Accessed April 15, 2019).

28 Transportation Security Administration *Advanced Integrated Passenger and Baggage Screening Technologies* (2017). https://www.dhs.gov/sites/default/files/publications/TSA - Advanced Integrated Passenger and Baggage Screening Technologies_0.pdf (Accessed August 15, 2019).

29 https://www.kaggle.com/c/passenger-screening-algorithm-challenge (Accessed April 15, 2019).

30 https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/DHS-CWMD-RDPA-18-0080-ROSA/listing.html (Accessed April 15, 2019).

this has been less common in mission delivery funded work (e.g., design of nuclear weapon systems). There are new, innovative development approaches being explored in mission delivery to promote rapid experimentation and learning by establishing a safe environment where innovators can rapidly test concepts and fail early with little consequences, so that failure later in the development cycle can be avoided. One example is the DOE National Nuclear Security Administration (DOE/NNSA) and Sandia National Laboratories HOTSHOT program,[31] where sounding rockets are used to provide realistic environments to test and qualify components of future weapon systems. The cost of this rocket program is modest and ensures that technologies are de-risked and prepared for large-scale testing on DOD systems.

Conclusion

Successful innovation is possible, but there are many building blocks. Success requires a holistic look at the R&D value-delivery chain to include people and culture, technologies and capabilities, and practices and operations. There is a strong level of innovation present in the U.S. that could be leveraged by the national security industrial base; however, there are a number of barriers due to processes, procedures, culture, and organizational structures that inhibit effectively harvesting and shaping those innovations. A number of potential solutions have been presented, but many more are needed to revitalize key parts of the R&D value-delivery chain and unleash innovation across the national security industrial base.

31 https://www.energy.gov/nnsa/articles/nnsa-conducts-rocket-based-research-hawaii-hot-shot (Accessed April 15, 2019).

Goals and Metrics for Innovation

Mona Dreicer

The Challenges

As has been emphasized in earlier chapters, the United States is grappling with a growing set of challenges on both a regional and global scale—increased major power rivalries, climate change, and environmental or political upheaval driving population migration are some examples. The National Defense Strategy Commission[32] has raised an alarm and more specifically outlined urgent challenges that must be addressed to maintain a strong defense of the United States. The report stressed the overarching need to position the U.S. military for success and the ability to defeat major power rivals in competition and war.

The Commission outlined seven general operational challenges that need to be addressed:

- Protecting critical bases of operations, including the U.S. homeland, forces abroad, and allies and partners;
- Rapidly reinforcing and sustaining forces engaged forward;
- Assuring information systems in the face of attack and conducting effective information operations;
- Projecting and sustaining U.S. forces in distant anti-access or area-denial environments and defeating anti-access and area-denial threats;
- Deterring and if necessary defeating the use of nuclear or other strategic weapons in ways that would fall short of justifying a large-scale nuclear response;
- Enhancing the capability and survivability of space systems and supporting infrastructure; and
- Leveraging information technology and innovative concepts to develop an interoperable, joint command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architecture and capability that supports the warfare of the future.

They applauded the National Defense Strategy[33] for stressing the need to pursue technological innovation to overcome the military's capability and operational challenges, in areas such as protecting critical bases of operation,

32 *Providing for the Common Defense. The Assessment and Recommendations of the National Defense Strategy Commission*, National Institute of Peace, Washington, DC (2018).

33 Summary of the 2018 National Defense Strategy of the United States of America. Department of Defense, Washington United States (2018).

assuring information systems, conducting effective information operations, defeating anti-access–area-denial threats, deterring enhancing the capability and survivability of space systems and supporting infrastructure, and developing interoperable joint C4ISR.

The NDA Commission urged strengthening the U.S. National Security Innovation Base and the pursuit of *technological innovation* that can be introduced into operation in an aggressive manner. This has translated into a call to the U.S. technical community to "out-innovate" our adversaries and formulate "disruptive science and technology" that can significantly bolster our national security in an era of strategic competition, with a focus on R&D to create new capabilities and concepts of operation, or devise significant improvement of the status quo.

But innovation is the means—not the ends—so clear objectives and metrics for success must be formulated. But to define effective metrics, goals, strategies, and priorities must be articulated first. Metrics must provide a means of measuring whether the benefits of innovation have achieved the desired outcome at a reasonable cost. A few of the authors in this document have addressed this issue in different contexts.

In setting out the ingredients needed to create an environment to foster innovation, Michael May begins with the need for "posing the right question." Whether innovation is to be applied to new or existing missions, one must know if the goal is to advance the state of the art or improve on an existing process, fill a gap or vulnerability, or design a completely new approach.[34] Even with a good strategy as a departure point, addressing the question of *how to get innovation right* regularly touches on the issue of metrics. Nerayo Teclemariam states: "The only meaningful metric of success is whether the end is achieved." In order to be effective, we must define the scope of the innovation domain.[35]

Paul Bernstein states that one of the requirements for a U.S. innovation strategy is "dynamic operational and strategic metrics that are meaningful for assessing qualitative advances in military capability and their impact on competition with other great powers." He advocates the development of metrics that "follow from the basic organizing principles for innovation; if we organize around a series of specific challenges framed by adversary advances that must be overcome to ensure operational success, then it should be possible to derive discrete measures of effectiveness relevant to assessing balances of power and our ability to keep adversaries at a disadvantage." [36]

Chuck Lutes further develops the importance of metrics—"metrics that could provide adequate measures of the progress made by each country. Development of useful metrics would be an important first step in understanding the nature of technological change in

34 See May chapter on *From Innovation to Capability: Lessons from the Past.*

35 See Teclemariam chapter on *The Building Blocks of a Successful Innovation Strategy.*

36 See Bernstein chapter on *"Innovating" versus "Out-Innovating:" Innovation as a Form of Strategic Competition.*

the context of strategic competition.[37] So, in this context, success must be measured in the context of competitors and rivals, not just in improving existing capabilities.

One of the key challenges to harness the results of innovation is to determine if the U.S. government should (or even could) control the pace and direction of innovation for national security. The USG must accept the need to tap into the natural evolution that is occurring in private industry, knowing that their drivers for innovation may be different.

Meeting These Challenges

To position the U.S. military for meet the challenges that have been outlined by the NDS and NDS Commission, innovation is needed in the three general areas of *operation concepts, technology*, and *acquisition and procurement*.

Innovative operational concepts will strive to maximize effectiveness of existing and emerging technologies to achieve "strategic advantage, including addressing the ability of aggressive regimes to achieve a fait accompli against states on their periphery, or to use nuclear or other strategic weapons in ways that would fall short of justifying a large-scale U.S. nuclear response."[38]

In support of the NDS, the undersecretary for defense for research and engineering (USDR&E) established ten priority *technology* domains. Here is where technological innovation will be focused on: hypersonics; directed energy; command, control, and communications; space offense and defense; cybersecurity; AI/machine learning; missile defense; quantum science and computing; microelectronics; and nuclear modernization.[39] Protecting and strengthening the U.S. National Security Innovation Base, is seen as an essential step for successful technological innovation. But again, what exactly needs to be done for each type of technology and how will success be measured?

It is often noted that much of today's innovation is occurring in the private sector, so besides protecting the USG technology base and infrastructure and improving the USG processes for *acquisition and procurement*, building a better bridge for the efficient and cost-effective transition of concepts, methods and technologies from the private sector to the Department of Defense is an essential element.

37 See Charles Lutes chapter on *U.S. Defense Strategy and the Innovation Imperative*.

38 *Providing for the Common Defense. The Assessment and Recommendations of the National Defense Strategy Commission*, National Institute of Peace, page 26, Washington, DC (2018).

39 *Providing for the Common Defense. The Assessment and Recommendations of the National Defense Strategy Commission*, National Institute of Peace, page 26, Washington, DC (2018).

Metrics for Innovation

When considering the long list of national defense and warfighting needs requiring innovation, it is clear that there is no one-size-fits-all set of metrics that could possibly be applied. Definition of metrics will vary depending on the scope of the question or problem and the specific goals. In developing metrics, a useful construct forms when the goals across a range of innovation projects are grouped into the categories of: technical capabilities, infrastructure, operations (implementation), speed & efficiency, and cost savings. There are limitations, and these categories cannot be applied to defining metrics for innovation for all areas listed under operation concepts, technology and acquisition & procurement. Also, a system-wide assessment may be more appropriate than specific metrics for one technology or part of the process. Depending on the case, additional overarching evaluations may be needed to include assessing the impact on the balance of power and the ability to keep adversaries at a disadvantage.

The investment and risk associated with innovation to improve technical capabilities and infrastructure will vary depending on whether the goal is to produce a game-changing, disruptive, new capability or whether providing incremental improvements is sufficient. However, in both cases, possible metrics would measure general improvement (faster, better, and more efficient); successful solution of an existing problem; improved response to a new adversary capability; and successful technology transfer from R&D to production and ultimately the success in practical implementation.

Some of the more traditional metrics used are countable items such as the number of new patents, products, publications, record of inventions, increased savings or return on investment (ROI). These metrics may not provide a direct measure of support to U.S. national security, in response to adversary competition, for example, but can be viewed as useful metrics to evaluate the success of a technical project. For example, ROI can be a useful metric of overall success if the entire systemwide costs savings are included in the evaluation.[40]

The next generalized goal for innovation focused on process—such as improving operations over a wide range from acquisition and procurement to military deployment and operations. The metrics would be the same whether innovation is set to achieve incremental evolution or complete disruption. The same metrics useful for measuring improvements for technical capabilities would apply here, but implementation of the new process must consider how to maintain continuity of existing processes/operations. Effecting changes in an ongoing (and essential) process will be difficult. So, in addition to the earlier metrics outlined, one must consider simplifying and/or improving existing processes and institutional culture; the ability to overcome entrenched interests when implementing the new process; and elimination of paths to major failure should be added. If the innovation is dual-use, successful, sustainable technology transfer via a commercial pathway should be an additional metric.

40 See Teclemariam chapter on *The Building Blocks of a Successful Innovation Strategy.*

Increasing the speed and efficiency of existing or new capabilities/operations are goals applicable to projects associated with acquisition and procurement (for purposes of R&D and integrating innovation into the existing program); communication of vast amounts of data; data analysis; and ability to communicate results to decision-makers. To measure successful innovation for technical capabilities, the intended results must be compared to the optimal performance of the existing system and whether innovation meets or exceeds the minimum requirements.

Finally, a cost–benefit evaluation is needed of the new capability or process. For national security purposes, this must be considered in the context of U.S. military and Department of Defense requirements. If this is to be done properly, the complete system (life-cycle) must be considered, so that all potential costs and savings are included. Otherwise this metric will not be providing an accurate assessment.

Additional Considerations

An additional goal for innovation could be to foster cooperation with U.S. Allies, and train the next generation of experts. Government-to-government technical cooperation projects, between technically-capable peers, bring together partners with unique expertise and broaden the technical base in both countries. Such connectivity mirrors the current trend towards globalization in the private sector. A greater diversity of intellectual power is likely to spur innovation and broaden the horizons (and possible mindset) of a possibly isolated technical community. I believe that greater transparency into national security technology capabilities can also provide allies with more confidence in U.S. security and extended deterrence assurances and such programs can yield great benefits, ranging from improving cost-effectiveness to building long-term trusted relationships. Innovation in cooperative projects with U.S. allies, can build lines of communication that might pave the way for future strategic stability. But defining commonly accepted metrics for such cooperation has eluded us so far. Over the past 25 years, many international cooperative programs have struggled to define metrics, and experience has shown that qualitative metrics of success are not universally accepted. If the general view is that qualitative metrics have fallen short, possibly political science and international relations research can help formulate better metrics.

Looking towards the future, the U.S. and our allies need to ensure that the next generation of national security experts have the expertise required. Bright young minds are attracted to solving important national security challenges and if an "informed buyer" is ready to consume the results, and allows sufficient time and resources for trial and error, Mike May believes that a successful innovation environment will attract the next generation. Here, measuring success is a bit easier. Educational programs, graduation rates, funded internships and fellowships, and ultimately employment in the national security field can be tracked as a measure of success.

Getting Innovation Right in the Strategy for Long-Term Competition

Brad Roberts

A core function of the Center for Global Security Research is to bring together emerging communities of interest to generate new insights into new national security challenges. Since the release of the 2018 National Defense Strategy, the Center has tried to advance thinking about the goals of the strategy, the problems it identifies, and needed next steps. The commitment to "out-innovate" major power adversaries in a long-term strategic competition emerged as an obvious focus for this effort. The workshop we convened in spring 2019 compelled the participants to come to terms with the changing context, means, and ends of competition and also brought into better focus areas for additional work. As convenor of the proceedings, I took away a short list of key insights, as follows below. These are my personal impressions.

First, long-term competition with other major powers is inherently multidimensional. Competition is not limited just to the military dimension of the relationship. It is also economic, scientific, political, even ideological in character. The National Security Strategy takes this broader view, whereas the National Defense Strategy focuses primarily on the military dimension.

Second, innovation means something different in each of these dimensions. The different communities of interest use a common vocabulary to mean different things and thus sometimes miscommunicate. The goals of innovation vary across this multidimensional landscape, as do the obstacles to success and metrics. The S&T community has an approach to innovation that is not universally shared and even within that community private and public sectors are not necessary well aligned.

Third, in the U.S. strategy for long-term competition, innovation can play an important role in shifting the military balance in favor of the United States and its allies. But it cannot do so without a sound understanding of the problems that the military needs to solve. As the National Defense Strategy Commission concluded, that understanding is missing today. There is little understanding of the operational challenges facing U.S. and allied forces in a major regional war against Russia or China or of the ways in which existing or conceivable technologies might be utilized to address those challenges. There is little understanding of the operational challenges that the United States and its allies can or might be able to present to our adversaries or of the ways in which existing or conceivable technologies might be utilized to address those challenges. In the assessment of the NDS Commission, U.S. military planning and thus U.S. capability development plans are informed by a number of dangerously optimistic assumptions, including, for example, (1) that the U.S. will face a single military foe at a time, (2) that the U.S. homeland will be a sanctuary, (3) that the U.S. will have assured access to critical overseas facilities,

(4) that war with a major power adversary will be localized to its region, (5) that the U.S. and its allies will have air superiority, sanctuary in space, and information security, and (6) that the U.S. and its allies will be able to resupply their forces at war. Innovation at the conceptual level, at the operational level, and in capability development are essential to dealing with the reality of these flawed assumptions.

Fourth, the aspiration to "out-compete adversaries" implies a net assessment approach with Russia and China—whose strengths and weaknesses as competitors are often misunderstood in the U.S. Both are formidable competitors, though each has different strengths as innovators. Both have innovated at the strategic level of war and have achieved major reforms in defense and military strategy, in planning for all-domain regional war, and in exercising for such a war. Russia's innovative strength is its deep scientific culture. China's is its ability to generate and direct huge amounts of capital. It's no longer just a "fast follower;" it is moving into a leadership role. Despite decades of advocacy by Andy Marshall, net assessment remains an underdeveloped disciplined. But it is essential to understand how and how hard to compete. In the military domain, for example, simple comparisons of who possesses the more advanced technologies may not convey an accurate picture of who has better utilized technology to enable a particular strategy.

Fifth, successful strategies for innovation generally require:

- A high degree of motivation (in the military realm, a strong dose of fear or failure)
- Clear goals aligned with the right kinds of questions
- Sustained leadership focus
- A healthy irreverence
- The freedom to experiment and the time and resources to get it right while learning through failures
- Some metrics, but not too many or at the wrong time in the development cycle
- Organizational structures that are mission-focused and flexible.

Sixth, some organizations are capable of meeting these requirements for the long term, others succeed only for a single major cycle of war, and still others prove incapable of innovation. A critical discriminator of success is institutional culture: many organizations are averse to both risk and the changes necessary to become more open in identifying new opportunities and challenges

Seventh, successful innovation often involves partnerships outside the U.S. government. Overseas allies can play numerous important roles. They may have unique scientific or engineering expertise. They may be effective in coming to quick but durable decisions. They may be able to test in a more permissive environment than the U.S. Private-sector partners also play numerous important roles. The successful mobilization of private venture capital to enable startups and experiments has greatly helped refocus DOD interests. Bigger tech firms are stepping up. Further progress in developing these partnerships requires something more than ad hoc collaboration. As a starting point, it requires that government understand the culture and incentive structure of private-sector technology developers. This in turn requires programs that enable skilled and interested individuals to work in both public and private sector organizations over time, perhaps on a loaned basis.

Eighth, the federally funded research and development centers (FFRDCs) are also key partners. But their role is in flux. The changing national economy has altered the playing field and the rules of the game that dominated through the Cold War. Finding the new niche for the labs requires having some sense of the core competencies of the other actors on each playing field.

Ninth, Cold War successes in innovation cast a long shadow of expectation over the present period. Among Americans there is a widespread optimism that America and Americans excel at innovation and can readily adapt military competition to U.S. advantage. This may not be particularly well-founded. There are many sources of innovation in the U.S. economy but their application to the solution of military operational problems has been difficult to mobilize. DIUx demonstrated the potential of small-scale improvements. Moreover, the political polarization of the country obstructs many of the necessary new relationships, reduces the flexibility of the government in addressing new challenges, and is constraining the flow of resources.

Tenth and finally, the Department of Energy has much to learn from the Department of Defense about reforming for innovation. But DOD also has some things to learn from DOE. DOD's Strategic Capabilities Office and Defense Innovation Unit (formerly DIUx, x for experimental) illuminate the possibilities of tapping rapidly into the most dynamic sectors of the U.S. economy to field targeted solutions to current operational problems with available or close-to-market technologies. Like the IC, DOD has also been successful in mobilizing private equity for select solutions. DOE has been more effective at using its laboratory system to generate big breakthroughs of a kind that shift the capability net assessment in decisive ways. They have been successful in part because they've been given a mission and then left to do their job.

About the Contributors

Paul Bernstein is a distinguished research fellow at the Center for the Study of Weapons of Mass Destruction (WMD Center) of the National Defense University in Washington, DC. He is engaged in a range of policy support, research, and professional military education activities related to WMD, nuclear policy, deterrence, threat reduction, and regional security.

Madelyn Creedon served as principal deputy administrator of the National Nuclear Security Administration (NNSA) within the Department of Energy from 2014 to 2017. She also served in the Pentagon as assistant secretary of defense for global strategic affairs (2011–2014) and as counsel for the U.S. Senate Committee on Armed Services for many years beginning in 1990.

Mona Dreicer is deputy director of the Center for Global Security Research at Lawrence Livermore National Laboratory. Her substantive focus is on nonproliferation and treaty verification. Prior to joining the lab in 2003, she served at the U.S. Department of State as director of the Office of Nuclear Affairs.

C. Robert Kehler retired from the United States Air Force at the rank of general in December 2013 after almost 39 years of distinguished service. From January 2011 until November 2013, he served as the commander of the United States Strategic Command (USSTRATCOM).

Charles Lutes is the director of the Office of Defense Coordination at Lawrence Livermore National Laboratory. Prior to joining the LLNL he served as the director of the Center for the Study of Weapons of Mass Destruction at the National Defense University in Washington, D.C.

Michael Markey is a senior fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory, where he focuses on escalation control and strategic stability, with an emphasis on emerging domains of competition. Prior to joining the Lab he spent several years in the U.S. government studying national security issues, with an emphasis on arms control and nuclear nonproliferation issues.

Michael May is director emeritus of Lawrence Livermore National Laboratory, having served in that role from 1965 to 1971. He is also professor emeritus (in research) at Stanford University's school of engineering and a senior fellow with Stanford's Freeman Spogli Institute for International Studies. He served previously as co-director of its Center for International Security and Cooperation.

Brad Roberts is the director of Center for Global Security Research. Prior to assuming this responsibility in 2014, he served as deputy assistant secretary of defense for nuclear and missile defense policy (2009–2013). Prior to entering government service, Roberts was a research fellow at the Institute for Defense Analyses and earlier at the Center for Strategic and International Studies, editor of the Washington Quarterly, and an adjunct professor at George Washington University.

Nerayo Teclemariam is the manager of the Systems Research and Analysis Department within the Homeland Security and Defense Systems Center at Sandia National Laboratories.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory in part under Contract W-7405-Eng-48 and in part under Contract DE-AC52-07NA27344. The views and opinions of the author expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC. LLNL-TR-789113 TID-55668

Lawrence Livermore National Laboratory