"Challenges for Global Military Operations"

Presentation by Dr. Tom Allen,
Deputy Director, Studies and Analysis, Joint Staff J-8

to

8th Annual Disruptive Technologies Conference

November 8, 2011

Federal Gateway
Washington, DC

Thank you Dr. Kimmel. I appreciate your kind introduction and inviting me to speak this morning at the 8th Annual Disruptive Technologies Conference. As one of the first presentations of the morning, I have the opportunity to provide you with some context regarding the challenges facing the Defense Department in the coming years. I also appreciate speaking early in the lineup of presentations since it minimizes the chance that I will contradict something you have already heard. My plan this morning is to describe some of the fiscal, strategic and operational challenges facing global military operations, building on the challenges presented by Mr. Scharre, such as anti-access/area denial threats and capabilities, cyber challenges, and hybrid threats, to set the stage for thinking through how the United States can best respond. Most of that will be left to you, both at this conference and in the years to come. I would also like to share some of my ideas about how the Defense Department can address these threats by crafting responses and evaluating them through modeling and simulation prior to fully committing to detailed solutions in our future budgets. Those detailed solutions will require close coordination between the government and industry and must be undertaken with a better understanding of how to effectively transition S&T concepts to real military capability. Secretary Lemnios will talk more about that in his presentation, but aligning your research, to include IRAD, more closely to the challenges confronting the military will facilitate early access to Department research capabilities and will certainly help meet both the fiscal challenges that I will talk about this morning and better align concepts for transition. In a time of shrinking budgets, we can ill afford to divert funding to explore solutions that our research tells us up front that we will be unable to transition.

One of my responsibilities in J8 is to work with the Offices of the Under Secretary of Defense for Policy and the Cost Assessment and Program Evaluation to develop force planning

scenario constructs for the Department. These scenario constructs are built to represent multiple military operations or "demand signals" that must be integrated into a time-phased response. Before getting to the specific challenges, I'd like to describe one integrated defense scenario construct for you. First, imagine that the U.S. military is fully engaged in two simultaneous conflicts—these combat operations do not involve all U.S. ground forces but they are geographically separated and place a heavy burden on our logistics supply chain. Now, in the midst of these combat operations, suppose the United States becomes involved in a third military operation. Imagine that this operation includes a multi-national coalition built to enforce United Nations Security Council resolutions and protect innocent civilians. Assume that this third military operation involves kinetic force and requires substantial support from American aerial refueling and reconnaissance platforms. Finally, to make things even more interesting, imagine a last piece of this scenario construct involves a natural disaster which creates the need for a massive humanitarian response to help the victims of the catastrophe, much of this provided by the US military. Remember, in this scenario construct, all of these events are occurring with some degree of simultaneity, meaning they overlap to some extent in time, requiring our military response to be integrated to avoid mission failure. At this point I need to admit that this demanding situation was not a planning scenario cooked up by the Joint Staff to be used for future planning by the Department of Defense. I am sure most of you have already realized I am describing the real-world events from March of this year when the United States military continued combat operations in Iraq and Afghanistan, supported Operation Unified Protector in Libya, and responded to the terrible tragedy in Japan from the earthquake and tsunami. The point of relating this "real world" scenario is to emphasize that the Department of Defense cannot predict with precision the specifics of any future challenge. However, our goal is to

ensure that when the real challenges occur, the Department and the nation have enough military capability and capacity to respond to multiple overlapping challenges, such as those we experienced earlier this year, with minimal risk to the security of our nation.

Maintaining military capability and capacity for global military operations will become an ever-increasing challenge in the years ahead due to the current state of the U.S. economy and the requirement articulated at the national level to reduce government spending. As mentioned earlier, I work in J-8, which is the Joint Staff's Force Structure, Resources, and Assessments Directorate. As a result, I can't leave here this morning without conveying to you the serious fiscal challenges facing the Defense Department and the nation. General Dempsey, our current Chairman of the Joint Chiefs, has inherited a situation where it is clear that the budget for the Department of Defense will be reduced over the next several years and he is working closely with the Secretary and other members of the National Security Community to ensure that the available budget will be sufficient to allow the military to execute the National Military Strategy. As you are aware, the final size of the reduction is undetermined, but the President has already agreed to reduce defense spending by $450 Billion over the next 10 years. This reality matches the well-documented United States historical pattern of reducing defense spending at the conclusion of combat operations. For example, after funding reaching a peak in 1968, the post-Vietnam defense budget, adjusted for inflation, came down by over 30% by 1975. After the successful conclusion of the Cold War, there was a nearly identical reduction of 30% in defense spending in the 1990s. We followed similar patterns after the Korean War and World War II. Thus, following the conclusion of combat operations in Iraq this year and Afghanistan by 2014, we should anticipate and plan for a significant reduction in the defense budget.

The reduction in defense spending will affect almost every portfolio within the Defense Department. Secretary of Defense Panetta has already stated that the Department must look at "all areas of the budget" for potential savings. However, the search for more efficient ways to conduct the same business will yield only a limited amount of savings, and it's clear that the total amount we might save from just cutting overhead costs will not meet the current target. Thus, other elements of the budget, from force structure and procurement to research and development, will undergo a vigorous review. During the most recent drawdown in defense spending, in the period from 1991 until 2001, funding for procurement was reduced by about 50% while the Department managed to maintain investment for RDT&E at about the same level over that period of time. In this coming period of reductions, it is unlikely that a single portion of budget will absorb the bulk of the cuts or that any portion of the budget will be exempt. And because we know that a "peanut butter spread" of cuts across all portfolio areas, across all Services, across all capabilities, will result in a force that may not be able to conduct the highest priority missions we're going to have to think hard about how we approach this. A peanut butter spread would include force elements that are developed piece meal and without the necessary integration with other elements of the force. So we'll need to carefully asses our force structure, basing, posture, modernization, readiness level, and R&D options against sets of scenarios that represent the kinds of challenges we are likely to face; only in this way can we hope to make informed decisions that will allow us to measure the tradeoff between incurred risks and fiscal resourcing decisions. This may lead us to adjust our national strategic objectives to ensure we continue to operate within acceptable risk boundaries. In testimony to Congress last month, Secretary Panetta explicitly stated that "we must avoid a hollow force" and "maintain a military that, even if smaller, will be ready, agile and deployable."

It is within the context of these fiscal realities that we'll need to address some of the strategic security challenges facing the Defense Department. Over the last year, the new SecDef and Chairman, along with the Combatant Commanders, have been clear in articulating the threats and associated strategic/operational challenges they present in today's environment. We continue to confront the threat of terrorism. Regardless of what we've been able to achieve -- and we have achieved a great deal -- there remain real threats out there, not only in Pakistan but also in Somalia, Yemen, North Africa, the Philippines and other places – places where terrorists continue to plan attacks against our deployed forces and allies and, in some cases, against our homeland. In addition to terrorism that threatens our citizens and institutions, the United States will continue to have to deal with the potential proliferation and use of weapons of mass destruction, a specific goal articulated by some hostile organizations. WMD in the hands of terrorists threaten death and destruction on a scope that used to be associated only with a state enterprise. And the allure of nuclear weapons may cause small states to seek such a capability in order to give their desires for power and influence disproportionate influence, one reason why the US continues to oppose any attempts at nuclear proliferation. In the cyber world, technical capability within reach of a single individual has put at risk the information and process requirements of entire organizations and enterprises. DoD for one continues to confront both cyber attacks and an increasing number of those attacks on a daily basis, from individuals and from organizations. More specifically, as we move beyond combat operations in Iraq and Afghanistan, the Department of Defense will need to address a litany of strategic security challenges, such as:

- The threat to the United States and its allies posed by North Korean nuclear and missile capabilities, its proliferation of weapons of mass destruction and associated technologies, and its potential for instability
- Transnational violent extremist organizations (VEOs) undermine stability and threaten traditional Allies and emerging partners. We see this today along the southern border of the United States, but need to be alert for any symbiosis between extremist groups and other factions that, in the aggregate, tend to strengthen each other and which, if left unchecked, could threaten wider areas of territory and the stability of civilian governments.
- China's significant military modernization.
- Territorial disputes, and the increasingly assertive actions needed to resolve them, across a wide range of national borders, something that continues to generate conflict and instability. In fact, a few years ago I visited the UN and was reminded by some of my hosts that virtually every country in the world has some question with at least one of their neighbors regarding the true provenance of a specific piece of their current territorial structure.
- Increasingly persistent and sophisticated cyber threats that challenge unencumbered operations.

State and non-state actors operating with malign intent can readily exploit the conditions noted above, with the most dangerous scenarios involving a mix of insufficient governance, weapons proliferation – especially Weapons of Mass Destruction, the influence of hostile states, and the free flow of extremist elements across national borders as well as the ready accessibility of cyberspace to anyone who would use it for hostile purposes. As I

noted earlier, an individual actor in cyberspace can affect our national economy and security on a scale previously reserved only for nation states. The asymmetric nature of cyber warfare makes it difficult to apply traditional deterrence strategies and conventional doctrine to its exploitation. Other strategic challenges include:

- Transnational criminal activity - to include piracy and trafficking in narcotics and persons that reject the rule of law and challenge international order
- Humanitarian crises such as pandemics and famines, as well as natural disasters such as tsunamis, earthquakes, and volcanoes
- Environmental degradation caused by poor resource management, the pillaging of natural resources, and disputes over resource sovereignty

In addition to the "strategic" challenges that I've just enumerated, there are a number of operational challenges that currently face the Department; these are challenges that must be addressed within the overarching strategic context of fiscal constraints and preservation of appropriate military capability, but these operational challenges could prove to be so fundamental to what the military does that not addressing them could result in strategic failure.

Your conference is meant to tackle one such challenge head-on. Our military forces continue to transform to meet the hybrid threat we face in conflicts today and expect to face for the foreseeable future. By hybrid threats, I mean those that cut across conventional warfare, irregular warfare and cyber warfare. These may include attacks by nuclear, biological and chemical weapons, improvised explosive devices and information warfare. Basically, I'm talking about those potent, complex variations of warfare elements and the complex dynamics of the battlespace that requires a highly adaptable and resilient response. We have made huge strides in adapting our doctrine, tactics, techniques, and procedures to become more effective

against irregular forces and the asymmetric capabilities they attempt to employ to marginalize our conventional strengths. I applaud your purpose here today, as you seek to identify and promote the development of game changing technologies and the deployment of follow-on operational capabilities that will overmatch hybrid threats to U.S. military operations. One of the issues that "keeps me up at night" is that we as a military and a nation still do not have a theory explaining how fundamental factors drive insurgencies and instability in social systems, and so cannot rigorously assess the impact that existing or new capabilities across the spectrum of national power will have when applied in a particular way, in a particular situation, under specific conditions. Without such an understanding, we run the risk of misaligning scarce fiscal resources in the development of capabilities that could have marginal utility in situations we might face on a regular basis in the future. Luckily there may be some help on the horizon; more on that later.

Another operational challenge confronting the Department is the increasing ability of various state and non-state actors to deny us the freedom to operate in an area of operations, thereby denying us the opportunity to even attempt to achieve our objectives. To my mind, these actors are following the very path that you at this conference hope to follow: they look to leverage "disruptive technologies" to either deny us entry into the area of operations (referred to as Anti-Access), or to constrain our ability to operate within the area (known as Area Denial). Although in many cases we well understand the individual effects of these technologies that could be arrayed against us, in general we don't do a good job at looking at the big picture using the system-of-systems view that is necessary to fully capture the synergies the adversary hopes to leverage and potential cascading consequences on our own integrated capability that the adversary hopes to exploit. Without the capability to perform this holistic analysis, we are ill-

prepared to make capability development and resource allocations decisions that will be the key to posturing our forces to defeat Anti-Access/Area Denial threats in the future. Again, there is hope on the horizon here as well.

A third operational challenge, which also confronts us at the strategic level, is the threat posed by adversaries who have the capability to attack us through the cyber domain. As we look to leverage technology to gain an asymmetric advantage over our adversaries, we have come to rely more and more on our dominance in the realm of information technology. However, as we are frequently discovering, our doctrine and technology in this area are not yet on a par with our capability in the physical domains to defend ourselves from attack and retaliate to an attack if necessary. One might suppose that, since the cyber domain is composed of the various information technology systems, components, and connections that span the globe, it would be most amenable to analysis by computer modeling and simulation. However, similar to the problem we face in the Anti-Access/Area Denial challenge area, we currently have limited comprehensive means of holistically assessing red or blue capabilities and their interactions in the cyber domain. However, the Department is also taking steps in this area to rectify the shortfall.

I recognize that I have just touched on several challenges facing the Department, some of which we are only beginning to recognize as having the capacity to negate current military capability. Fortunately, the Department and its partners in industry and academia are looking at a broad array of potential actions and responses. If you remember nothing else from my presentation today, I hope that you'll keep in mind the underlying challenge we face: pursuing all options and then picking the winner after all the results are in is no longer possible. We need to develop a methodology that not only helps us to identify which of a number of threats are the

most probable and most dangerous, but also helps to determine which of an array of solutions will address a threat most appropriately—before the threat itself is fully manifested. We know that, in order to support strategic decisions that balance limited fiscal resources with acceptable risk, the Department has developed several different methodologies and processes. I'll describe two existing processes, and propose a third that I'd like to see adopted.

The first process, and the primary activity the Department uses to inform capability development, force sizing, and force shaping decisions for the mid-to-long-term -- in other words for that period that exists beyond the Fiscal Years' Defense Plan -- is our Support to Strategic Analysis effort, or SSA for short. The Department's force planning community has worked hard to lay the analytic foundations to support strategic analysis necessary for the decision support our institutions need in order to manage these challenges. Based on challenges raised in the last Quadrennial Defense Review, this effort has generated three integrated security constructs, or ISCs. The first ISC focuses on the emergence of a near peer competitor; the second addresses the challenges faced during two overlapping regional conflicts; the third looks at the requirements associated with maintaining a rotational force engagement capability, much as we have for the last decade in Afghanistan and Iraq. While these challenges are giving way to a newly articulated national security strategy, by understanding the requirements for a force that could be called upon to prevail in any one of these three challenge spaces, we have developed a sound basis for examining aspects of the emerging strategy. Our current scenario library addresses these challenges under a number of different conditions – objectives, constraints, limitations and assumptions. Moreover, we have invested time and resources into creating an initial set of operational solutions (CONOPS/Force Requirements) against these ISCs which serve as starting points or baselines for DoD strategic analyses and assessments. Coming out of

the last Quadrennial Defense Review, we have also created detailed, model-based integrated data sets to enable the community to engage in more robust analyses to understand the implications and phenomena behind some of the challenges I have outlined. As you work with specific military customers to develop capability and plan for its transition, you need to take advantage of the existence of these scenarios and products, which are available to the planners and programmers of the community, in order to help advance the body of knowledge regarding policy and force planning analyses. Your contribution to advancing that body of knowledge is essential, for we are just beginning to understand these challenges well enough to adequately model and emulate their affects for planning purposes.

A second process which actually forms the basis for a more focused effort that we are engaged in is the development of what the US Transportation Command and the Defense Logistics Agency are calling the Comprehensive Materiel Response Plan or CMRP. In this era of decreasing defense budgets the Department must more thoroughly examine how it does "business" across the spectrum of military operations. One of the legacy constructs that is being examined is the forward positioning of material to support combat operations, known as Pre-positioned Materiel, or "PREPO". At the direction of the Vice Chairman and supported by the Secretary of Defense's Efficiencies Task Force, TRANSCOM and DLA, together with the Joint Staff, the Combatant Commands, and the Services, are developing a new construct intended to transform how the Department approaches Material Distribution. The goal for the CMRP is to achieve the integration of materiel posture and distribution management to support the full range of military activities. To do this the CMRP must provide agile, flexible, and responsive solutions across the full range of military activities. Solutions must be capable of effectively supporting the War fight and also efficiently supporting the rest of military operations encompassing

everything from partnership exercises to major disaster relief efforts. The CMRP must also leverage shared capabilities and common materiel to create joint solutions. This mean we must examine what we deploy, how we deploy it, and how often we deploy it Basically, CMRP will answer the question, "What do we need to routinely move when we deploy, support an exercise, or provide disaster relief?" and then achieve synchronized planning, effective sourcing, and optimized positioning through enterprise management. A long range goal of the CMRP is to gain total asset visibility of what is required for the most dangerous situations we might face, in addition to determining what is routinely deployed to address the most likely situation. With this knowledge the CMRP will provide efficiencies by developing an enterprise management structure that will more efficiently manage the materiel distribution system.

The goals for CMRP are challenging but necessary to posture the Department's materiel response program to effectively and efficiently support the nation during this time of decreased resources and ever-present challenges. I see modeling and simulation as a way to better evaluate the challenges of this specific effort as well as to test the options available for meeting those challenges. The analysis team is currently in the process of developing an appropriate M&S environment to better inform the Department on understanding and meeting the CMRP challenges.

While Support to Strategic Analysis and the CMRP processes provide specific responses to a range of challenges confronting the United States, a third, possible, response to the strategic challenges we face is to develop an approach that takes a systematic, rigorous, analytic approach to investment across the entire spectrum of military capability requirements. Our British allies are already embarked upon just such an initiative, which they refer to as their Strategic Balance of Investment, or "Strat BOI" process. We currently have in place multiple processes, key

expertise, and data sets that would be vital in the creation of such a process here in the United States. However, our scenario sets and the data that accompanies them are not nearly robust enough yet to support such a comprehensive attempt; and currently, the Department is finishing up specific scenario sets to support time-sensitive decisions for the upcoming FY14 POM, so Departmental decisions needed to "fill in" the scenarios required to span the entire decision space is still a ways off. Assuming the Department did decide to embark on a Strategic Balance of Investment initiative, we would also need to create the rule-sets for combining scenarios as well as for quantifying risk, and we'd have to adapt analytic methodologies to generate outcomes in the desired form. The latter issue is much less problematic than it might have been a decade ago, since there are a number of capable linear and nonlinear program applications in existence that are well-suited to this kind of optimization problem, using fiscal constraints to inform the objective function. The former issue of creating appropriate rule sets is thornier. As anyone who has spent time working around the Department of Defense knows, reaching consensus on business rules is often the biggest challenge one faces when attempting to conduct analyses with far-reaching implications. And we still find the quantification of risk to be one of the most challenging aspects of any capability analysis. Nevertheless, I strongly feel that unless we move aggressively to develop this kind of overarching capability to provide our senior leaders the kind of decision support they need and deserve, we'll have missed a major opportunity when we attempt to allocate our resources wisely to cover the situations we could face in the future without incurring unacceptable risk.

I mentioned before that I am concerned about investments to meet the challenges of hybrid adversaries or irregular warfare without sufficient information about the fundamental driving factors in these conflicts. Lack of this information prevents us from creating models to

represent system behavior, which in turn makes the creation of simulations of the full Irregular Warfare operational environment impossible. I firmly believe that we need these kinds of simulations to enable us to explore the potential impacts of new technologies and doctrine, and application of whole-of-government approaches that leverage all the instruments of national power. While we are currently pursuing the knowledge and gathering the necessary data needed to develop useful models and simulations in the hybrid threat arena, our lack of understanding about the populations that are the focus of most hybrid warfare operations makes it impossible to reasonably test alternative approaches to the problem. How will our presence influence the success of specific actions or projects in the area? Are these projects or the reality of US armed presence in a region the reason for the observed effects? What will happen when the projects continue and US soldiers are no longer visible? I have found that there is no universal answer to any of these questions, but knowing the right framework for a specific situation will help planners and commanders develop successful operational plans and concepts of operation for the situations that they face. Knowing when the conditions exist for appropriately applying the requisite tools or simulations is as important as developing those tools and simulations to move our cause forward in this area.

This means that we technologists, analysts and engineers will need to pay more attention to the human dimension of any issue involving the use of the nation's military forces. In order to understand these dimensions, the Department has at least three initiatives in place: the Human, Social, Culture, and Behavior (HSCB) Modeling Program sponsored by the Assistant Secretary of Defense for Research and Engineering; the Irregular Warfare Modeling & Simulation High Level Task, an effort sponsored by the M&S Steering Committee led by AT&L; and the Minerva Initiative. All of these are all good examples of the Department's efforts to better

understand and model human behavior. And we need to understand human behavior in the context of a specific threat in order to understand when a specific military option will be appropriate. The HSCB invests in research to generate capability through the development of a knowledge base, building models, and creating training capacity in order to understand, predict, and shape human behavior cross-culturally. This is the starting point for generating appropriate human behavior representation in our operational tools.

The IW M&S High Level Task promotes the development of tools, models, methods, and data to support irregular warfare practitioners in areas including data collection and management, relevant theory, validation and standards, collaboration, and the establishment of a modeling and simulation as-is baseline. While neither the HSCB nor the IW M&S High Level Task has been long in existence, in theory, the High Level Task should provide the baseline insight and information for not only developing more useful tools to support operators confronting hybrid threats, it should also provide the sweet spot in which HSCB efforts can thrive.

The Minerva Initiative is a Department-sponsored, university-based social science research initiative launched by the Secretary of Defense in 2008 focusing on areas of strategic importance to U.S. national security policy. The goal of Minerva is to improve DoD's basic understanding of the social, cultural, behavioral, and political forces that shape regions of the world of strategic importance to the U.S.. The research program provides basic information by leveraging and focusing the resources of the Nation's top universities, analogous to the Cold War development of Kremlinology and game theory. And while it seeks to define and develop foundational knowledge about sources of present and future conflict with an eye toward better understanding of the political trajectories of key regions of the world, it also should provide basic

information that the HSCB program, the IW M&S High Level task, and DoD's partners can use to generate more useful tools for planners and operators confronting the hybrid threat.

The second operational problem I mentioned, that of Anti-Access/Area Denial, has senior DoD leaders rightfully concerned. Because of our inability to realistically simulate, and hence come to a holistic understanding of this kind of environment, we do not know how an adversary might leverage multiple capabilities to magnify our operational obstacles or how we might be able to overcome those obstacles with the right application of technology and doctrine. That in turn means we do not fully understand the implications of critical, costly resourcing decisions, nor can we provide the comprehensive analytical insights needed to fully inform those decisions. To address this shortfall, the Department plans to integrate current disparate "system-on-system" simulation architectures into single integrating "systems-of-systems" architecture transitioning away from many stand-alone simulations to a single integrated threat simulation which covers all war fighting domains. This Integrated Threat System Modeling & Simulation (ITSMS) will:

- Represent the variety of integrated threat systems in A2/AD environment
- Develop authoritative analysis of threat "systems-of-systems" for use across DoD
- Improve fidelity and scalability of current threat analytic capabilities
- Integrate architectures from across IPCs to produce threat "systems-of-systems" analysis
- Integrate existing and emerging M&S architectures to perform integrated kill chain analysis
- Produce a common threat system architecture to foster re-use; support threat and blue analysis
- Support live, virtual and constructive stand-alone and distributed simulations

Authoritative threat representations to support the communities enabled by M&S

- Develop a capability to analyze threat Systems-of-Systems in an A2/AD environment
- Develop architecture to enable both Red and Blue analysis

We are also moving aggressively to develop a virtual cyber environment that will enable multiple simulations to interact within a common context to enable system-of-systems analysis of both blue and red capabilities, their interactions, and the impact of new technologies and doctrines. The Cyber Operations Research & Network Analysis or CORONA is an M&S research effort that if successful will enable the user to ascertain cyber effects of an attack and the resulting impact on a mission; create a cyber operations assessment environment; enable heterogeneous, scalable assessments; portray advanced cyber threats and representative environments; and integrate with other live virtual constructive (or LVC) components, in order to obtain operational "so what?" answers.

My goal this morning was to present some of the challenges facing the Defense Department in order to give you context for the presentations and discussions over the remainder of your conference. In the Department, we are wrestling with a range of challenges starting with the constrained budget environment, but including the strategic and operational challenges we face in this environment such as anti-access/area-denial, hybrid warfare and cyber threats. I have described some of the ways the Defense Department is working to address these challenges. This audience, more than most, understands that we do not have all the answers and we must continue to leverage the creative genius and innovation of both those in the National Security Sector and our partners in Academia and Industry to help us meet these challenges. In fact, we need to work closely not only on solutions, but on determining early which solutions will have the broadest impact and start near the beginning of their life cycle to figure out the most efficient pathway for transition. As I stated at the start of my comments, we cannot predict where exactly

the future challenges will come from, but we know they are coming. With your assistance, we will continue to identify the key challenges and ensure the military maintains the capability and capacity to preserve and protect our nation's security in the face of these challenges.

Thank you.

I am prepared to take questions from the audience and, although my prepared remarks are not classified, I can respond to your questions up to the SECRET level as required.