Strategy Research Project

Strategic Technology

by

Captain James E. Boswell
United States Navy

United States Army War College
Class of 2012

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*
11-03-2012

2. REPORT TYPE
Strategy Research Project

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE

Strategic Technology

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Captain James E. Boswell, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Colonel David R. Arietta
Department of Command, Leadership, and Management

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This paper examines the concept of technological surprise and offers insights as to where future investments might most be needed. Analysis of recent trends and studies on technological surprise present a rich resource for development of analytical criteria to evaluate current efforts toward preventing or overcoming technological surprise. The analytical criteria are then used to evaluate the current organization and strategy of the United States Navy in this area. Finally, recent historical examples of technological surprise are evaluated against this analytical scheme to develop potential areas for improvement. This paper argues for a systematic, approach to technology analysis, awareness and information sharing. It examines the expansion and investigation of massive multi-player gaming environments to facilitate expert education, collaboration and experimentation. Finally, it recommends a focus on red team analysis and experimentation as a means of minimizing strategic surprise from technological sources. To fully explore potential strategic futures DOD must adopt a systematic approach to ensure education, collaboration and experimentation amongst operational, scientific and technical intelligence expert communities.

15. SUBJECT TERMS
Adaptability, acquisition, futures, planning, intelligence, experimentation, technology surprise, surprise, technological surprise, collaboration, innovation, research

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	38	**19b. TELEPHONE NUMBER** *(include area code)*

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

USAWC STRATEGY RESEARCH PROJECT

STRATEGIC TECHNOLOGY

by

Captain James E. Boswell
United States Navy

Colonel David R. Arrieta
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Captain James E. Boswell

TITLE: Strategic Technology

FORMAT: Strategy Research Project

DATE: 11 March 2012 WORD COUNT: 7,265 PAGES: 38

KEY TERMS: Adaptability, acquisition, futures, planning, intelligence, experimentation, technology surprise, surprise, technological surprise, collaboration, innovation, research

CLASSIFICATION: Unclassified

This paper examines the concept of technological surprise and offers insights as to where future investments might most be needed. Analysis of recent trends and studies on technological surprise present a rich resource for development of analytical criteria to evaluate current efforts toward preventing or overcoming technological surprise. The analytical criteria are then used to evaluate the current organization and strategy of the United States Navy in this area. Finally, recent historical examples of technological surprise are evaluated against this analytical scheme to develop potential areas for improvement. This paper argues for a systematic, approach to technology analysis, awareness and information sharing. It examines the expansion and investigation of massive multi-player gaming environments to facilitate expert education, collaboration and experimentation. Finally, it recommends a focus on red team analysis and experimentation as a means of minimizing strategic surprise from technological sources. To fully explore potential strategic futures DOD must adopt a systematic approach to ensure education, collaboration and experimentation amongst operational, scientific and technical intelligence expert communities.

STRATEGIC TECHNOLOGY

The Department of Defense (DOD) spends extraordinary effort, time and money considering future challenges, and the environment in which they will occur. This is likely no different from the efforts of political and military leaders from the time of Themistocles; it is in fact basic to the concept of civilization. For a civilization to survive, it must consider future challenges, prepare for winter, for example, or more specifically, prepare for war. But unlike the challenges leaders faced in 500BC or even 1942, current leaders face a pace of technological and societal change that is so broad and rapid it defies understanding. Dr. George Heilmeier in a 1976 article for Air University Review pointed out that the key to *surprise* "is in the recognition or awareness of the impact of technology and decisiveness in exploiting it."[1] In Dr. Heilmeier's view then, surprise is the gap between technological change and doctrinal understanding and integration. If it is accepted that the rate of technological progress is accelerating, then the influence of technology on possible future scenarios must be seen as increasing. Due to this, the world has become both smaller and infinitely larger during the last two decades; challenging our ability to understand it conceptually and practically. It has become smaller in the familiar sense of the "shrinking planet." For example, individuals from all walks of life, religion and ethnicity have unparalleled physical and intellectual access to one another and, more importantly, to the ideas, knowledge, and concepts that span humanity. One no longer has to master the Urdu language to read the local newspaper from Attock, Pakistan,[2] for instance. It is accessible in a variety of languages on any mobile device with a data-link. This also shows how the world has expanded. Not only is there nearly unlimited access to knowledge and data, but we have created a new domain, cyberspace, that theoretically, at least, has no permanent limits. Paradoxically, cyberspace has created unique opportunities for adversaries and new forms of access not limited by physical proximity. Cyberspace and wireless technology have also made possible commercial off the shelf (COTS) command, control, communications, and intelligence systems.

These technologies, and many others like them, represent a growing challenge to DOD's capability to understand and prepare for current, developing and future challenges. Given the nature of defense planning and programming, there is an unceasing pressure to define the future operational environment and adversary scenarios. Yet, as the Joint Operating Environment (JOE) 2010 points out, the pace of change across demographics, science, society, and many other areas makes these potential futures quite difficult to understand with much clarity. These accelerating trends leave us with one sure prediction, and that is for the increasing potential and scale of technological or capability surprise in the future. Recent history has ample evidence of this trend and points with some clarity to effective approaches that could minimize the potential for technology surprise and reduce its impact.

Strategically, we have guidance to prepare for a wide range of potential scenarios from defeating Al-Qaeda to neutralizing weapons of mass destruction. Specifically, with regards to surprise, we are directed to build forces and capability that are "adaptable." Despite pervasive guidance to strive for adaptability, DOD has struggled to either predict technology shifts or to adapt quickly and efficiently when confronted with technology surprise.

Strategic guidance since 1990 reveals a growing understanding of increasing strategic uncertainty and risk of doctrinal or technological surprise. Since that time, there have been numerous instances of technological surprise that have in turn led to significant efforts to understand and analyze its origins and character. The Defense Science Board study on Capability Surprise[3] and other studies on technological or capability surprise offer consideration of best practices and decision processes to minimize its potential impact. An alternate approach to consider is through the lens of successful historical efforts to achieve technological surprise. These examples show how this type of surprise was accomplished and provide insights to strategic choices that might minimize or prevent them. All of the services have an array of organizations focused on preventing this type of strategic setback. For brevity, the U.S. Navy organization and strategy will be examined. Recent examples of technology surprise will serve as contrast to examine what kind of failures have been experienced even with current organizational and strategic approaches and perhaps understand where efforts to improve should focus.

Background

U.S. strategy has gradually shifted focus during the last two decades due to the demise of the Soviet Union, the continued extensive U.S. involvement in the Middle East, international anti-terrorism efforts, and global efforts to restrict the influence and reach of international "bad-actors." The demise of the Soviet Union continues to represent a strategic discontinuity for the U.S. in the sense that strategic thinkers and planners no longer have a crisp focus on the primary threat. The U.S. is no longer engaged in a calculated competition with a near-peer competitor, in which both sides shift their capabilities investments based on careful study and analysis of a primary adversary. Instead, the defense enterprise finds itself struggling to define the most likely nature of future strategic threats and, correspondingly, to define the nature of operational challenges. Some believe that future operations have a strong likelihood of resembling either of the last decade's counter-insurgency efforts in Iraq or Afghanistan. Others emphasize that we rarely refight the last major conflict and find reasons to focus on potential near-peer competitors and more conventional combat operations.

Cold War strategies were by necessity threat-based, largely due to the relatively well defined nature of the primary adversaries and their military, operational and technical capabilities. During the last two decades, the Department of Defense strategic guidance has shifted from the Cold War threat-based paradigm to a capabilities-based paradigm. This started immediately following the fall of the Soviet Union with Secretary of Defense Dick Cheney stating "we are building defense forces today for a future that is particularly uncertain, given the magnitude of recent changes in the security environment."[4] He goes on to write "we are striving to provide a future President with the capabilities five, ten or fifteen years from now to counter threats or pursue interests that cannot be defined with precision today."[5] This uncertainty continues today and is reflected in all current strategic guidance from the Joint Operating Environment 2010 (JOE) to the most recent National Military Strategy 2011 (NMS).

Strategic Guidance

In the forward to the JOE 2010, General James N. Mattis takes pains to emphasize the speculative nature of efforts to define future environments and challenges. We do this, he says, to ensure we "think through the nature of continuity and change in strategic trends to discern their military implications."[6] The context of his comment is that, while our speculation will have only limited success, the exercises of analysis, scenario development and course adjustment are crucial to the process of "services adaptations."[7] The JOE focuses on the time frame of 15 to 25 years in the future and stresses repeatedly the difficulty of precisely predicting future challenges and environments. Paradoxically, as Richard Danzig points out, "the U.S. military relies on prediction to forecast needs and influence the design of major equipment." [8] Prediction is central to DOD capability requirements, acquisition, and budgeting efforts, yet we are in an era where prediction efforts are becoming less reliable, while development and acquisition timelines continue to lengthen. DOD interest and focus on technology surprise is driven by a relatively new environment where "technology and globalization have empowered first- and second-tier states, non-states, and even individual extremists alike."[9] This new environment has given the potential for WMD or WMD-like effects to many actors beyond the traditional "great nations." Also, growing interdependencies from social to cultural to technical make the understanding, analysis and prediction of unrest extremely difficult.[10] In the final analysis, the demise of the Soviet Union has reduced the international focus on the "great conflict" and created a broad array of security challenges which stress the nation's capacity to analyze, predict or prepare for an uncertain future environment.

The strategy to minimize the impact of technological surprise hinges on improving U.S. ability to innovate and adapt. The Quadrennial Defense Reviews (QDRs), since 1990, still place significant emphasis on a combination of predictive scenarios to provide context. The 2010 QDR emphasizes ongoing efforts to win today's wars and it provides future focus through eight descriptive challenges.[11] While this list does not represent threat-based planning, it can be assessed as something of a mix of capabilities-based planning and threat-based planning. While it is clearly anchored in the current fight and current strategic requirements, the 2010 QDR provides guidance in broad terms that can be interpreted to cover the spectrum of future conflict and engagement.

Technology Surprise

Francis Fukuyama, in his introduction to the book *Blindside,* summarizes recent events saying "the past decade and a half has demonstrated that nothing is as certain as uncertainty."[12] While he was not focused specifically on technology, his statement captures the growing trend of uncertainty in international affairs that can, in part, be traced to the pace and scale of capability and technological advancement. The Defense Science Board (DSB), in its *2008 Summer Study on Capability Surprise*, categorized surprise into two distinct groupings: known surprises and surprising surprises.[13] The DSB identifies known surprises as those for which potential, evidence and consequences are readily available and clearly understood.[14] For these types of surprise, the U.S. could and should have been prepared, but failed to take adequate measures. These are the types of surprises that Heilmeier and Mahan referenced as preventable through thorough study and experimentation.[15] Surprising surprises, according to the DSB report, are those for which evidence and consequences are much less clear.[16] An example of this is the successful use of advanced mathematics by the Allies during World War II to decipher Axis communications.

Another approach to defining surprise comes from the National Research Council (NRC) in its report from a recent symposium on the subject:

Type 1: A major technological breakthrough in science or engineering.

Type 2: A revelation of secret progress by a second party which may have an unanticipated impact.

Type 3: Temporal surprise, when a party makes more rapid development or advancement in a particular technology than anticipated.

Type 4: Innovative technology applications, such as using an airplane as a weapon, or increasing the lethality of improvised explosive devices.[17]

This delineation of surprise has been endorsed by the Defense Intelligence Agency's (DIA) Defense Warning Office (DWO) and will be used to examine and understand various scenarios of technology surprise.

In the book, *Managing Strategic Surprise*, the authors do not define surprise, but focus instead on the idea of risk. Risk they define as the product of likelihood and consequences and they approach the idea of risk by examining how it is managed in other disciplines.[18] This approach to surprise is especially relevant as it closely correlates to the recommendations of the DSB on capability surprise. The authors of this study contend that this systematic examination of requirements, combined with a study and understanding of the necessary convergences, could provide significant focus to investment in research and development areas. In his book on surprise, Meir Finkel advocates technological and doctrinal surprise as primary categories, saying "the importance of the technological dimension has surpassed the operational."[19] He goes on to explain that the increasing pace of technological progress leads to an expanding divergence of timing and complex interaction that is difficult to forecast.[20] Interestingly, this point of view is not supported by recent U.S. experience with improvised explosive devices (IEDs) or with other technology surprises such as advanced 4th and 5th

generation fighter capabilities. In each of these cases, the technology was not the cause of surprise as much as doctrinal integration and implementation.

In his book on the concept of innovation, Stephen Peter Rosen urges us to keep a distinct separation between the ideas of "technological innovation" and "behavioral innovation."[21] Technological innovation is defined as "the process by which new weapons and military systems are created," except where new technologies drive organizational adjustment.[22] This is an important concept when examining past examples of technological surprise, from the perspective of understanding how they were accomplished and how to best avoid them.

Convergences

For another perspective on technology surprise, the U.S. Army's STAR21 (Strategic Technologies for the Army of the Twenty-First Century) researchers examined the methodologies used to make specific technological forecasts for the U.S. Army and made recommendations to adjust future efforts.[23] They also reviewed similar studies conducted by the U.S. Navy and U.S. Air Force and determined that all three sets of studies had used similar methodologies. The major findings of this study were twofold. First, they found that "forecasting is difficult due to the unpredictable nature of technology and often exponential technological advances."[24] Secondly, that the nature of the exponential technological surprises that forecasting efforts had failed to predict were tied to the concept of "technological convergences".[25] The definition of convergences is inexact but can be summarized as "the confluences – of individual sciences and technologies that could enable"[26] surprising technological capabilities.

The STAR21 study recommends a methodical approach to studying convergences related to specific warfighter capability requirements; however this same concept could be effectively focused on examining potential new threat capabilities and vectors. The approach used would be to determine a continuum of near, mid, and far term operational requirements. An iterative approach is recommended using subject matter experts (SMEs) to first determine the end state capabilities required for far-term mission sets. Then the SMEs would study actual operational capabilities (regardless of science and technology maturity) matched to the end states, and finally devolving operational capabilities into base science and technical breakthroughs that must be achieved.[27]

Related to the STAR-21 finding, the United States Marine Corps (USMC) Warfighting Lab has experimented with an innovative methodology for examining disruptive technologies called "commercial hunter" or commercial technology assessment (CTA).[28] This approach focused teams of college students on prescribed Marine Corps scenarios that incorporate detailed U.S. capabilities and gaps. The teams were tasked to combine readily available (had to be mature within 5 years) technologies in innovative ways to produce unexpected threat vectors. The initial test of this approach was considered to be a success in that the teams produced imaginative and effective solutions.[29] Two additional CTAs have been conducted subsequently and there is evidence that this approach offers an effective methodology for discovering potential new threats. Notably, the CTA effort represents confirmation of the STAR-21 reports recommendation and perhaps a model for service based technology assessment. Addressing technology assessment (TA) from the perspective of ethical considerations, Richard Sclove highlights various approaches similar to that of Commercial Hunter, further validating this concept.[30] What is not clear is what would be the best combination of comprehensive approaches to capture layperson, potential adversary, and professional military assessments that inform doctrine, tactics, and capability acquisition decisions.

The STAR-21 report and the “commercial hunter” effort illuminate two distinct ways that convergences can be effectively examined. STAR-21 developed the methodology and necessity for internally focused assessment, with future capability potential and requirements as the focus. The STAR-21 effort used operationally knowledgeable and tactically proficient SMEs along with expert knowledge of future technical capabilities to examine potential capabilities. The USMC study pointed to another aspect of this type of study, which is using a study group that is relatively less experienced in military operations and tactics to examine how future technologies and capabilities might be used to undermine expected U.S. capabilities and doctrine.

Robert McCreight, of the George Washington Institute for Crisis, Disaster, and Risk Management, argues persuasively for a national Technology Assessment (TA) mechanism.[31] He points out that the commercial potential of rapid advances in “biotechnology, nanotechnology, plasma physics, materials science, space science, propulsion dynamics, and artificial intelligence” among many others combined with the global economy means that rapid change is inevitable.[32] His recommendations include national and international TA mechanisms, but are more aimed at identifying potential technologies for government sponsorship. This aspect of TA should be monitored by DOD analysts but may not meet the specific needs of military doctrine, strategy, and capabilities assessment. Specifically, Dr. McCreight’s recommendations call for an open and transparent process that informs the international as well as national community.

This type of effort, while laudable for reasons of international stability, peacekeeping, and health would likely reduce the critical military advantage that such analysis might provide. For DOD purposes, TA efforts that include blind studies and classified studies may be more valuable and desirable since vulnerabilities and advantages might be revealed during these processes.

Dr. McCreight provides a useful definition of technology assessment:” the systematic evaluation of innovative, novel, and unique discoveries and developments in all fields of science and technology to examine both the immediate and long-term societal, political, and ethical impacts of new ideas and advancements to ascertain whether their impact is either positive or negative.”[33] A modified definition may prove more useful for DOD purposes: the systematic evaluation of discoveries and developments in all fields of science and technology to examine both the immediate and long-term strategic, operational, and tactical impacts to current capabilities, strategies, and doctrine.

Probably the most comprehensive recent effort to examine technological surprise was the Defense Science Board’s 2008 *Summer Study on Capability Surprise*. While the DSB definition of capability surprise is slightly different than that for technology surprise provided by the NRC, their recommendations and finding are useful for this discussion. The DSB study recommended a five step process to manage surprise:

1. A scanning and sifting process that narrows the many possibilities to the most worrisome few

2. A “red” capability projection function that takes a “deeper dive” on the worrisome few through analysis, simulation, experimentation, and/or prototyping
3. A net assessment process in which the deeper understanding of “red” gained through capability projection is played against blue capabilities in order to assess the degree to which the nation can address the threat or adapt capabilities already in hand
4. An options analysis team to provide an unbiased evaluation—or “rack and stack”—of the alternatives should blue capabilities prove inadequate
5. An ability to produce a decision package that can be acted upon by senior leadership[34]

These recommendations coincide with and expand on the proposed DOD definition of technology assessment. It is significant, however, that the DSB study emphasized the need for a major red teaming capability. This coincides with expert recommendations compiled in the findings of the 2009 National Research Council Symposium on technology surprise.[35] One of the speculations of the keynote speaker at this event was on how information technology might be used to facilitate the “sharing of ideas” across broad audiences of differing educational and experiential backgrounds.[36] While the speaker did not delve into this subject, it is worth examining in some detail. One of the difficulties experienced in technology assessment is well documented in a full reading of the book, *Winning the Next War*.[37] In the last three chapters the author examines the problem of managing technology surprise. One of the key issues he uncovers is the need to share cultural and experiential knowledge across critical communities of experts. For military technology, these communities are the operational, scientific, and technical intelligence communities. How this expert knowledge can best be shared, disseminated, and used to establish understanding of critical decision spaces remains inexact. However, modern information technology might provide solutions that remain relatively untapped.

Examination of various aspects of technological surprise related to electronic warfare and armored warfare during WWII provides ample evidence for two recommendations. First, as Stephen Rosen has documented, sufficient adversary technical intelligence must drive military capability development.[38] U.S. development of ordnance and armor capabilities prior to WWII progressed with little or no understanding of the adversary, resulting in significant technological and doctrinal advantage for Axis forces. On the other hand, later in the war, significant understanding of German radar and radio technology led to a decisive U.S. and British advantage in electronic warfare.[39] Allied understanding of how Axis forces were using the electro-magnetic spectrum contributed significantly to development of effective jamming and radar capability and doctrine. These efforts were partially responsible for the defeat of the Axis bombing campaign against Great Britain.

In his examination of approaches to manage uncertainty, Dr. Rosen compares potential approaches. He makes a strong case for a "hedging strategy," that pursues a broad research approach investing in "the development of many different weapons up to the point where their costs and military performance" can be understood.[40] This approach methodology provides depth and context to the "net assessment" process recommended by the DSB. Another recommendation that this approach assumes is comprehensive experimentation that facilitates the understanding of military performance and implications for strategy and doctrine. As an example of hedging, he outlines how the U.S. used this strategy starting in 1946 to develop understanding of the decision space for strategic guided missile technologies.[41] This hedging strategy was particularly successful given the extremely poor understanding of the operational scenarios for strategic nuclear weapons. It set the stage for concrete production and further development in the mid 1950s that would establish and maintain U.S. advantage in nuclear weapons capacity and technology for the next 40 years.

These efforts provide a useful discreet set of recommendations for strategies that can be used to minimize and mitigate technology surprise:

- Convergence analysis that leverages expert communities (operational, scientific research, and technical intelligence) to examine and prioritize potential game changers
- Red Team convergence analysis that examines unexpected combinations of technologies that lead to disruption
- Net assessment or experimentation, which examines both red and blue options to develop understanding of potential future disparities
- Leveraging information technology to capitalize on broad range of expertise, education, and experience (operational, scientific, intelligence)
- Sufficient technical intelligence to understand adversary current and intended capabilities

These recommendations provide a potential lens through which service strategy, organization, and implementation of technology surprise mitigation and prevention can be viewed and perhaps effectively evaluated. While a full analysis of DOD strategy and organization is outside the scope and scale of this paper, analysis of a single service's efforts will provide a benchmark for these proposed strategies.

Navy Technology Assessment and Experimentation

Having examined the idea of technology surprise, how is DOD organized to prevent it and what, if anything, can be done to improve our posture? All of the services and the joint community have specific organizations whose goals include preventing technological and doctrinal surprise, but for brevity, this paper will examine the U.S. Navy's organization and strategy.

The Office of Naval Research (ONR) is the Department of the Navy's lead in sponsoring scientific research and its "mission, defined in law, is to plan, foster, and encourage scientific research in recognition of its paramount importance as related to the maintenance of future naval power, and the preservation of national security; and to manage the Navy's basic, applied and advanced research to foster transition from science and technology (S&T) to higher levels of research, development, test and evaluation."[42] ONR publishes its plan of execution in the "Naval S&T Strategic Plan" which lays out how it "sponsors research efforts that will enable the future operational concepts of the Navy and Marine Corps."[43] ONR's S&T vision is spelled out in four basic mission areas:

- Pursue revolutionary, game-changing capabilities for Naval forces of the future
- Mature and transition S&T advances to improve existing Naval capabilities
- Respond quickly to current Fleet and Force critical needs

- Maintain broad technology investments to hedge against uncertainty and to anticipate and counter potential technology surprise[44]

ONR's investment portfolio is overseen and managed by a hierarchically nested system of boards that starts at the Vice Chief of Naval Operations (VCNO) and Assistant Commandant of the Marine Corps (ACMC) level and ends with direction to the Director of ONR. This board system is meant to ensure that ONR investments are focused on operational priorities, while still ensuring a broad base approach to future technology requirements.[45]

In general, the demand signal for ONR comes from Navy and Marine Corps staffs (such as 2nd Fleet or 3rd Marine Amphibious Group), fleet or force enterprises (such as NAVAIR, NAVSEA) and "other" stakeholders. The introduction to the "Naval S&T Strategic Plan," emphasizes the need for increasing the engagement levels of senior Navy and Marine Corps leadership in the S&T process.[46] To summarize, ONR can be viewed as having the Department of the Navy mission to foster and develop new and future technologies and for organizing and prioritizing current technology challenges.

The Navy Warfare Development Command (NWDC) is "the Navy's champion for the rapid generation and development of innovative, game changing solutions in concepts and doctrine to enhance maritime capability at the operational level across the full spectrum and enable seamless integration in the joint and coalition arena."[47] In this role, NWDC has the Navy lead to develop and integrate capability at the operational level and shape current and future force employment through its "core competencies:

- Innovative concepts generation and development that is collaborative in nature and anticipates the requirements of and serves our primary customer the Fleet.
- Outstanding design and execution of experimentation and exercises with accompanying observation and analytical rigor that informs the continuum of gap analysis and solutions development.
- State of the art, forward leaning modeling and simulation to enable the Navy's end to end training continuum and assist with future force development.
- Dynamic Lessons Learned applied rapidly and logically to effect solutions in training and doctrine.
- Authoritative and well written current doctrine that is user friendly and enables clear, concise command and control and unity of effort."[48]

NWDC therefore provides leadership, organization, and integration for experimentation efforts within the Navy and for naval capabilities within the Joint environment. An important core competency listed for NWDC is its "innovative concepts generation" competency. This function, along with the role of experimentation and innovation, partially answers what much of the research on technology surprise recommends as a mitigating strategy. It appears from the NWDC mission statement that this effort is primarily focused on looking at technology integration and doctrinal development, but does not cover the "red" aspect of challenging U.S. Navy capabilities and doctrine.

The Naval War College (NWC) has a primary mission of using gaming, analysis, and research to help define the future Navy and its roles and missions. The primary goals of these efforts are to “anticipate future operational and strategic challenges; develop and assess strategic and operational concepts to overcome those challenges; provide analytical products that inform the Navy’s leadership and help shape key decisions.”[49] In this role, the NWC serves as the Navy’s premier war gaming center, providing high quality gaming, analysis of results, and research to understand potential futures. NWC uses collaborative as well as individual research efforts to include various dedicated research groups to develop understanding of current and future warfighting issues.[50] A review of the publications and research efforts available at NWC shows significant investment, analysis and focus on both “blue” and “red” technology use. From a scholarly aspect, the NWC clearly provides intellectual challenge of current doctrine and speculation and analysis on the impact and significance of future technological developments. It is unclear what level or frequency of systematic review of technical intelligence or technology assessment is used to facilitate the ongoing research and analysis.

Approaching innovation from another direction, the Chief of Naval Operations (CNO) has established the Strategic Studies Group (SSG). The SSG’s primary mission is to generate “revolutionary naval warfare concepts.” These concepts, are by definition, the kind that would upset the existing order of capabilities and doctrine, and would be non-consensual to operational forces. In this role, the “SSG focuses its efforts on warfighting concepts that appear to have great potential, but Navy organizations are currently not pursuing.”[51] The SSG was formed in recognition of the fact that many past successful innovations were brought about by “the iteration of thought between operators, technologists, and analysts.”[52] The CNO receives input from the SSG directly, then selects and directs implementation for the most promising revolutionary concepts. The SSG is meant to accomplish the sharing of expert understanding between operational, technical intelligence, and scientific experts to address complex operational challenges. In this role, the SSG works hand in hand with NWDC to develop and integrate conceptual proposals into Fleet Battle Experiments (FBEs), which seek to challenge and/or validate revolutionary ideas.

While there are many organizations involved in Technical Intelligence for the U.S. Navy, the Farragut Technical Analysis Center leads the way on strategic scientific and technical intelligence (S&TI). This center coordinates or conducts S&TI analysis of foreign capabilities, foreign material exploitation, signal intelligence analysis, modeling and simulation, and acoustic intelligence. Part of its mission is to provide information and services across the scope of Navy acquisition managers, weapons and systems developers, operational forces, and national security policy-makers.

To summarize, the overall U.S. Navy strategy and organization to prevent technology surprise appears to be well developed when compared to the recommendations of recent studies and experts. It arguably has multiple "convergence analysis" efforts from multiple levels of operational expertise, at least focused on improving U.S. capabilities. The Navy has a dedicated organizational investment in technical intelligence, with a focus on informing appropriate communities of decision makers and analysts. With NWDC, it has focused experimentation and concept development for U.S. capabilities. Finally, through the mechanism and focus of the SSG and NWC, the Navy has scholarly research, review, and analysis of adversary technological and conceptual futures. Despite all of this effort and focus, has the Navy managed to largely prevent technological surprise, or is there still room for improvement?

Signs of Failure

A recent and well documented example of technological surprise stems from the U.S. experience in Iraq since its invasion in 2003. The emergence of improvised explosive devices as a crucial tool for Al-Quada in Iraq and the Iraqi insurgents was a significant technological surprise for the U.S. military. After the coalition efforts during Operation Joint Endeavor in 1997, one of the lessons learned was that the use of IEDs could be a critical insurgent/guerilla tactic.[53] And there was significant scholarly work dedicated to the premise that indirect means of offensive weaponry, such as booby-traps or IEDs, would play an important role in guerilla tactics and strategy.[54] From Southwest Asia to South America, insurgencies during the 1990s used IEDs as one of their primary offensive weapons. While the use of IED's is properly considered a tactic, the effect in this case was strategic. U.S. forces quickly shifted operational focus and tactics, but many U.S. capabilities were not adequate to the new challenges of counter-insurgency. From the survivability of wheeled and tracked vehicles, to detection capabilities and procedures, to understanding and controlling/exploiting the electro-magnetic spectrum U.S. forces had systematically underestimated the environment.

When setbacks began to occur in Iraq, the U.S. was slow to develop a strategic response. From the time of Ambassador Paul Bremer's fateful decisions in May of 2003 to "de-Bathify" the Iraqi government and disband the Iraqi military, it took only a few short months for clear signs of a mounting insurgency to develop.[55] From this time, September and October 2003, it took a little over three years for the U.S. military and political leadership to come to grips with the scale, scope and context of the insurgency and implement an effective strategy.[56] What started as technological surprise resulted in extended doctrinal surprise which almost proved to be the U.S. undoing in Iraq.

But in contrast, understanding and adaptation to the IED threat began almost immediately. By July of 2004, DOD had initiated the Joint IED Defeat Task Force to bring together various efforts toward defeating the IED threat. This organization was transitioned to the Joint IED Defeat Organization (JIEDDO) in February of 2006. What is remarkable about this effort is that by March of 2007, insurgent IED emplacement efforts had increased by a factor of six while IED casualties had actually declined.[57] While the U.S. experience with IED's appears to be a clear instance of technological surprise, it also demonstrates the U.S. capacity to adapt and respond to surprise. The resulting rapid fielding of sensor, electronic warfare, armor upgrade, and various other IED defeat capabilities, represents a remarkable and successful effort to protect U.S. troops and defeat an adversary's primary offensive weapon.

The technique and lethality of the IEDs in Iraq represents an example of NRC Type-4 technology surprise, innovative use of technology. The potential critical failure here appears to be primarily a combination of failure of technical intelligence and red team experimentation.

A recent example of technology surprise in the aviation realm is the relative performance of the Indian Air Force SU-30 MK/MKi versus U.S. 4th generation fighters. U.S. understanding of this capability began at COPE INDIA 2004, a bi-lateral training exercise conducted at Gwalior in central India. During this exercise, U.S. fighters performed surprising poorly against a combination of Indian SU-30, Mig-29, and Mig-21 aircraft in air-to-air training exercises. At the time, the Chief of Air Combat Command commented that “we may not be as far ahead of the rest of the world as we thought we were.”[58] While some of the technical details of this event remain classified, subsequent description of the event detail various “exercise-isms” that contributed to the poor U.S. performance. Primarily, U.S. fighters were restricted to visual range missile shots or guns, and were engaged at a disadvantage of 3 to 1. While these might seem like un-realistically biased restrictions, it is important to understand that even under these circumstances U.S. fighters and pilots were expected to outperform Russian 4th generation fighters and Indian pilots. Four years later, India again exercised the SU-30 during the U.S. Air Force’s Red Flag exercise. During this exercise, the SU-30 MKi was deployed but was restricted to using its advanced radar in a training mode and restricted from using its electronic warfare suite.[59] With these restrictions, the aircraft and aircrew still performed comparatively well, fighting U.S. 4th generation fighters to relative parity.[60] This case appears to represent both technological surprise and doctrinal surprise because India’s Air Force (IAF) pilot training level and tactics and SU-30 MKi capabilities were unexpectedly advanced. Since both U.S. and Indian participants in this exercise were constrained from using full combat capabilities, such as certain aspects of electronic warfare and acquisition radar, it is too soon to draw definitive conclusions about the SU-30 MKi capabilities. The exact capability level of the SU-30 MKi remains unknown, but the demonstrated flight characteristics and avionics might be considered to constitute a Type 3 and possibly a Type 4 technology surprise. Another critical advantage of U.S. fighters in this exercise was their use of fully integrated network-centric capabilities, whereas the Indian fighters were limited to onboard radar, electronic warfare, and voice communications.[61] Even if U.S. technical intelligence on SU-30 MKi accurately documented the aircraft's capabilities, and comparable characteristics to U.S. 4th generation fighters, the reaction of the U.S. military aviators seems to demonstrate, at a minimum, a failure to communicate that intelligence. This revelation has implications for U.S. capability matchups with China and any other Russian customers and raises concerns about current U.S. fighter capability acquisition strategies. While the U.S. has maintained what is considered a decisive technical advantage in the air-to-air role with the F-22, the acquisition strategy for the F-22 may make the U.S. vulnerable to mass quantities of the exponentially less expensive SU-30 MKi.[62] In addition, China and Russia have also demonstrated what are considered to be 5th generation fighter capabilities, leading to potential technical parity over time.[63]

In another example of recent technological surprise, the Peoples Republic of China (PRC) has developed the "Anti-Access/Area-Denial" (A2AD) strategy to reduce the access and influence of U.S. military power in the East Asia sphere of influence. This strategy combines unexpected advances in technical capacity (Type-2) and unexpected combinations of technology (Type-4) to provide the PRC with a new capacity to challenge U.S. control of sea and air spaces. The most powerful example of technology surprise by China is in the development, testing, and fielding of guidance technology for long range ballistic weapons. The potential for this type of guidance was understood within the U.S. weapons development community, but the PRC was not expected to have the capacity to develop and field operational capability. As understanding of PRC capability deepened during the 2002-2010 timeframe, the U.S. Navy found itself unprepared to defend against a potentially devastating weapons technology. This example of technology surprise appears to have been caused by a combination of poor technical intelligence and poor understanding of adversary decision spaces. A combination of better technical intelligence that accurately captured Chinese developmental capacities or better "red team" analysis may have generated this as a likely approach. The ballistic guidance technology, sensor technologies, and other A2AD systems could have been captured with a combination of shared technology analysis awareness and adversary red team analysis.

What is revealing with these examples is that they confirm Dr. Heilmeier's definition of surprise as the "difference in the recognition or awareness of the impact of technology and decisiveness in exploiting it."[64] These examples support the advice of Alfred Thayer Mahan, writing on the subject of surprise in 1894, that surprise can be remedied by "careful study of the powers and limitations of the new ship or weapon, and by consequent adaptation of the method of using it to the qualities it possesses."[65] Modern warfighters must make an art of this "careful study" recommended by then Captain Mahan. Where the operational art, science, and technical intelligence of potential technology choices were once within the cognitive capacity of a small group or even a single individual, the vast modern spectrum of potential choices require integration of complex specialist knowledge.

Another aspect of these examples of technology surprise is that the most damaging surprises, for instance IED use in Iraq or guidance technology for ballistic weapons, were not major technological breakthroughs (Type 1). They were Type 4 and Type 2 or a combination thereof. One could argue that the primary means to mitigate a Type 2 surprise would be technical intelligence. In essence, we would have to have special knowledge of the adversary's decisions and/or technical focus. But, are these necessarily a failure of technical intelligence, or could these surprises stem more from a failure to understand the adversary's position and understand his strategic technology choices? For instance, in the case of China, could a combination of red team assessment and technology assessment have developed a better comprehensive understanding of their decision space and provided a focused understanding of likely choices and focus? At a minimum, such an analysis would have added context to known technical intelligence and could have kept U.S. capabilities ahead of potential adversaries.

Recommendations

Type 1 technology surprise remains a potential threat, but analysis of the U.S. Navy's organization and strategy shows that this is already the primary focus of the research and development community. The Navy is well positioned to prevent or mitigate this type of technology surprise investing over 45 percent of its research and development dollars in broad fundamental research.[66] A review of the recent studies and analysis on technology surprise failed to provide any recent examples of strategically significant Type 1 technology surprise.

A comparison of recent examples of technology surprise to the "discreet recommendations" developed earlier is useful in order to identify potential focus areas and approaches for reducing the potential and severity of technology surprise. Two conclusions can be gleaned from the Type 2 and Type 4 examples discussed earlier.

The first observation is that these examples reveal a need to have a deep understanding of the adversary's technical and operational viewpoint. Where technical intelligence might be unobtainable, a logical framework of adversary decision spaces and likely choices could provide additional focus for future U.S. technology investments. Whether and to what extent this type of analysis is conducted and integrated within the DOD and USN technology assessment decision processes is not clear. The value of this analysis would be to provide a critical secondary sensing system for adversary technology strategies. Where technical intelligence fails to provide critical understanding, convergence analysis, combined with a “red team” approach, might serve as a second system of understanding.

The second observation is that in order to have understood the potential for technological surprise from IEDs or ballistic guidance technology, DOD needed a way to experiment with and assess these potential adversary capabilities. This is an example of “net assessment and experimentation;” one of the discreet recommendations for avoiding or mitigating technology surprise. The Navy Warfare Development Command (NWDC) fulfills the experimentation and concept development role for the Navy, but does not appear to focus on adversary perspective. That is to say, NWDC’s experimentation role is primarily focused on integrating new capabilities and experimenting with improvements in existing and future U.S. capabilities and concepts. What does not appear to be well developed within the U.S. Navy architecture is an organization focused on “red team” experimentation. Analysis of the recent recommendations on technology surprise shows a need for an organization that finds and experiments with concepts, technologies and techniques that defeat friendly capabilities and concepts.

Examination of the findings and recommendations of the various studies on technology surprise reveal a repeated theme of utilizing information technology to help solve the problem of cross pollination across diverse groups of experts. For instance, ONR is currently experimenting with an IT approach to collaborative analysis. ONR's Office of Innovation has established the Massive Multiplayer Online Wargame Leveraging the Internet (MMOWGLI) to enable large scale, broad participation in technology assessment events. While this effort is in the early stages of experimentation, it will provide further understanding of the potential of networked approaches to provide cross-domain education, experimentation and learning. For example, forecast technologies, materials, or weapons can be integrated within a virtual environment that operational, scientific, and technical intelligence professionals "play" in. This environment might provide the platform to examine how either tactical professionals or technically proficient novices (such as college students) might use a particular technology in innovative ways. From another perspective, it could be used to garner insight from the disparate expert communities of operational art, technical intelligence, and research and development. Facts and assumptions about the utility of a potential technology or capability could be tested and experimented with while research efforts are still in the earliest stages. Another use of this type of networked game environment might be to examine how relative novices would use technology in novel ways to overcome existing capability mismatches, similar to the Commercial Hunter experiments, but on a larger scale.

Conclusions

Recent symposiums, studies and articles on technology surprise might lead one to the conclusion that DOD is poorly postured to understand, mitigate and prevent this strategic game changer. However, many of the insights and recommendations on technology surprise have already been integrated into the U.S. Navy strategic approach to this subject. These insights may still prove useful in examining the broader DOD architectures of research and development, technical intelligence and concept development. Nonetheless, examination of recent and historical examples of technology surprise provides potential areas for improvement. Red team approaches to convergence analysis and experimentation do not appear to be well developed aspects of U.S. technology strategy. Variations of gaming environments may provide a means of eliciting cross-domain expert participation to drive "novel intersections and complex interactions of ideas which would not"[67] otherwise occur. None of the approaches described here could, by themselves, prevent technological surprise. However, a systematic approach with multiple, mutually supportive processes of analysis and experimentation will better position DOD to minimize the instance and impact of technological surprise.

Endnotes

[1] Dr. George H. Heilmeier, "Guarding Against Technological Surprise", *Air University Review,* September-October 1976, 1.

[2] Attocknews.com Website, http://www.attocknews.com/ (accessed 03 Dec 2011), or Onlinenewspapers.com, http://www.onlinenewspapers.com/pakistan.htm (accessed 04 Dec 2011).

[3] Defense Science Board, *Report of the Defense Science Board 2008 Summer Study on: Capability Surprise Volume I Main Report* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Jan 2011).

[4] Richard B. Cheney, *Defense Strategy for the 1990s: The Regional Defense Strategy* (Washington DC: Department of Defense, 1993), 7.

[5] Richard B. Cheney, *Defense Strategy for the 1990s: The Regional Defense Strategy, 7.*

[6] Gen J.N. Mattis, *The Joint Operating Environment 2010* (Norfolk, VA: United States Joint Forces Command, February 2010), Forward.

[7] Gen J.N. Mattis, *The Joint Operating Environment 2010*, Forward.

[8] Richard Danzig, *Driving in the Dark: Ten Propositions About Prediction and National Security* (Washington DC, Center for a New American Security, October 2011), 5.

[9] Defense Science Board, *Report of the Defense Science Board 2008 Summer Study on: Capability Surprise Volume I Main Report*, 7.

[10] Ibid, 7.

[11] Robert M. Gates, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, 2010), 15.

1. Defeating Al Queda and its allies
2. Supporting a national response to attacks on, or natural disasters in, the U.S.
3. Defeating aggression by adversary states
4. Locating, securing, or neutralizing weapons of mass destruction
5. Supporting and stabilizing fragile states facing threats from terrorist and insurgent groups
6. Protecting American citizens in harm's way overseas
7. Conducting effective operations in cyberspace
8. Preventing human suffering due to mass atrocities or large-scale natural disasters abroad

[12] Francis Fukuyama, ed, *Blindside* (Baltimore, MD: Brookings Institute Press, 2007), 1.

[13] Defense Science Board, *Report of the Defense Science Board 2008 Summer Study on: Capability Surprise Volume I Main Report*, viii.

[14] Ibid.

[15] George H. Heilmeier, "Guarding Against Technological Surprise", 1. Alfred Thayer Mahan, *The Influence of Sea Power upon History* (New York, NY: Dover Publications, 1987), 22.

[16] Defense Science Board, *Report of the Defense Science Board 2008 Summer Study on: Capability Surprise Volume I Main Report*, viii.

[17] Committee for the Symposium on Avoiding Technology Surprise for Tomorrow's Warfighter, National Research Council, *Avoiding Technology Surprise for Tomorrow's Warfighter: A Symposium Report* (Washington, DC: The National Academies Press, 2009), 9-10.

[18] Paul Bracken, Ian Bremmer, and David Gordon, eds, *Managing Strategic Surprise: Lessons from Risk Management and Risk Assessment* (Cambridge, United Kingdom: Cambridge University Press, 2008), 4.

[19] Meir Finkel, *On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield* (Standford, CA: Stanford University Press, 2011), 46.

[20] Ibid.

[21] Stephen Peter Rosen, *Winning the Next War* (Ithaca NY: Cornell University Press, 1991), 5-7.

[22] Stephen Peter Rosen, Winning the Next War (Cornell University Press: Ithaca NY, 1991), 185. Mr. Rosen goes on to explain that organizational concepts such as amphibious warfare, COIN, strategic bombing, etc, are necessarily different than the development of carrier aviation, escort fighters, or helicopter warfare.

[23] Board on Army Science and Technology, Commission on Engineering and Technical Systems, and National Research Council, *STAR 21—Strategic Technologies for the Army of the Twenty-First Century* (Washington, DC: National Academy Press, 1992); Naval Studies Board and National Research Council, *Technology for the United States Navy and Marine Corps, 2000–2035* (Washington, DC: National Academy Press, 1997); Air Force Scientific Advisory Board, *New World Vistas, Air and Space Power for the 21st Century*, (Washington, DC: The Department of the Air Force, The Pentagon, 1995).

[24] John Lyons, Richard Chait, and Simone Erchov, ed., *Improving the Army's Next Effort in Technology Forecasting* (Center for Technology and National Security Policy: Fort McNair, Washington DC, Sep 2010) 28.

[25] Ibid.

[26] John Lyons, Richard Chait, and Simone Erchov, ed*., Improving the Army's Next Effort in Technology Forecasting*, 2.

[27] John Lyons, Richard Chait, and Simone Erchov, ed*., Improving the Army's Next Effort in Technology Forecasting*, 28.

[28] Director of Innovation Newsletter, March 2010, http://www.onr.navy.mil/en/Science-Technology/Directorates/office-innovation/~/media/FACADC6BD36D4027A9AB59153BAB42A9.ashx (accessed 01 Dec 2011).

[29] Director of Innovation Newsletter, March 2010.

[30] Richard E. Sclove, "Reinventing Technology Assessment," *Issues in Science and Technology* 27 No1 (Fall 2010).

[31] Robert McCreight, "Technology Assessment: Democracy's Crucible, the Future of Science and Technology, and Implications for Our Defense in the Twenty-first Century", *Strategic Studies Quarterly* (Summer 2010), 10-12.

[32] Ibid, 9.

[33] Ibid, 7.

[34] Defense Science Board, *Report of the Defense Science Board 2008 Summer Study on: Capability Surprise Volume I Main Report*, xii-xiii.

[35] Committee for the Symposium on Avoiding Technology Surprise for Tomorrow's Warfighter, National Research Council, *Avoiding Technology Surprise for Tomorrow's Warfighter: A Symposium Report* (Washington, DC: The National Academies Press, 2009).

[36] Ibid, 43.

[37] Stephen Peter Rosen, Winning the Next War.

[38] Stephen Peter Rosen, Winning the Next War, 187-189.

[39] Ibid, 220.

[40] Ibid, 244.

[41] Ibid, 245.

[42] Office of Naval Research, http://www.onr.navy.mil/en/About-ONR/science-technology-strategic-plan.aspx (accessed Jan 04, 2012).

[43] Office of Naval Research, *Naval S&T Strategic Plan* (Arlington, VA: Office of Naval Research, Sep 01, 2011), 1.

[44] Ibid.

[45] Ibid. ONR's investment portfolio is overseen by the Navy S&T Corporate board which includes the Assistant Secretary of the Navy for Research, Development and Acquisition (ASD-RDA) the Vice Chief of Naval Operations (VCNO) and Assistant Commandant of the Marine Corps (ACMC). This four-star board provides oversight and guidance to the Chief of Naval Research (CNR), assists in shaping the investment portfolio and approves Innovative Naval Prototypes (INPs). At the three-star level the Technology Oversight Group (TOG) provides for integration and assessment across the Future Naval Capabilities (FNC) program. The TOG ensures that "FNC investments are aligned to warfighter needs and fully coordinated to address identified capability gaps and properly planned to eliminate duplication of effort and to facilitate transition." The TOG is co-chaired by the Deputy Chief of Naval Operations for Integration of Capabilities and Resources (CNO N8) and the Commanding General, Marine Corps Combat Development Command (MCCDC). The TOG prioritizes Navy S&T investments annually and ensures they focus on Navy and Marine Corps requirements. It improves S&T transitions through additional senior leadership visibility and provides a critical linkage of S&T to requirements and the transition of S&T technology efforts to acquisition.

[46] Ibid.

[47] Navy Warfare Development Command, https://www.nwdc.navy.mil/Pages/AboutNWDC.aspx (accessed 04 Jan 2012).

[48] NWDC Facebook page, http://www.facebook.com/notes/nwdc-navy-lessons-learned/our-mission-vision-and-lessons-learned-program/291162354101 (accessed 04 Jan 2012).

[49] Naval War College webpage, http://www.usnwc.edu/About/Missions.aspx (accessed 05 Jan 2012).

[50] Naval War College webpage, http://www.usnwc.edu/Departments---Colleges/Center-for-Naval-Warfare-Studies/Warfare-Analysis-and-Research.aspx (accessed 05 Jan 2012).

[51] Naval War College webpage, http://www.usnwc.edu/About/Chief-Naval-Operations-Strategic-Studies-Group.aspx (accessed 05 Jan 2010).

[52] Ibid.

[53] Brian M. Breen, William C. Schneck Jr., "Operations and Training, A Road Fraught with Danger: Lessons in Mine Clearance", *Janes Interantional Defence Review Vol 30, Issue 11* (Nov 1997).

[54] Anthony James Joes, *Modern Guerrilla Insurgency* (New York, NY: Praeger, 1992).

[55] Keith L. Shimko, *The Iraq Wars and America's Military Revolution* (New York, NY: Cambridge University Press, 2010), 173-177.

[56] Ibid, 194.

[57] Joint Improvised Explosive Device Defeat Organization, *Joint Improvised Explosive Device Defeat Organization Annual Report 2006* (Washington, DC: U.S. Department of Defense, 2006), 15.

[58] The Associated Press, "General suggests U.S. dominance of skies may wane", *USA Today*, http://www.usatoday.com/news/washington/2004-06-23-us-skies_x.htm (accessed 12/30/2011).

[59] India Defence Webpage, "Exercise Red Flags: Indian Air Force Su 30 MKI Fighters Operated with Handicaps", *India Defence* (http://www.india-defence.com/reports-3988, accessed 02/19/2012).

[60] Lt Col Terrence Fornoff, (http://www.youtube.com/watch?v=w91FEykjlUg (accessed 12/30/2011), This video of Lt Col Fornoff discussing the performance and characteristics of SU-30MKi vs F-15C has him describing strengths and weaknesses of both aircraft and concluding that the overall engagements resulted in relative parity, depending on pilot skill and engagement mode.

[61] India Defence Webpage, "Exercise Red Flags: Indian Air Force Su 30 MKI Fighters Operated with Handicaps", http://www.india-defence.com/reports-3988, (accessed 02/19/2012).

[62] Mackenzie Eaglen, "Mind the Gap", *Proceedings Magazine* Sep 2010 vol 136/9/1,291 (Annapolis MD: U.S. Naval Institute, Sep 2010), 18.

[63] David Donald, "China Heads Out to Sea", *Aviation International News Online*, 15 Feb 2012, http://www.ainonline.com/aviation-news/singapore-air-show/2012-02-15/china-heads-out-sea (accessed 19 Feb 2012). See also, "PAK-FA at MAKS Airshow", *SP's Aviation*, Sep 2011 (New Delhi India: Athena Information Solutions).

[64] Heilmeier, "Guarding Against Technological Surprise", 1.

[65] Alfred Thayer Mahan, *The Influence of Sea Power upon History* (Dover Publications, New York, NY, 1987), 22.

[66] Office of Naval Research, http://www.onr.navy.mil/en/About-ONR/science-technology-strategic-plan.aspx (accessed Jan 04, 2012), 4.

[67] Melody Cook, Office of Naval Research, MMOWGLI Factsheet, emailed to author, Jan 15, 2012.