2018 Summer Study on
Strategic Surprise

June 2019

This report is a product of the Defense Science Board (DSB).

The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Depart of Defense (DOD).

DEFENSE SCIENCE BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON DC 20301-3140

MEMORANDUM FOR THE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

SUBJECT: Final Report of the Defense Science Board (DSB) Study on Strategic Surprise

We are pleased to submit to you the final report of the 2018 Defense Science Board Summer Study on Strategic Surprise. The study was chartered to do a "quick look" at what potential technical capabilities may not be sufficiently acted upon by the Department in the decade to come, that will lead to U.S. regrets in 2028. The report offers important considerations for the Department in response to future threats to our nation's security.

The study considered a wide number of topics and focused on ten areas of highest potential for regret in 2028. The ten areas include (1) defense against ballistic and cruise missiles; (2) defense against insider threats, and (3) defense against autonomous systems. They also include (4) superiority undersea and (5) superiority in the information environment. Also prioritized were (6) resilience of the U.S. defense industrial base; (7) resilience of U.S. positioning, navigation, and timing; and (8) resilience of the U.S. electrical grid. Two critical enablers were also identified: (9) biology and related technologies and (10) maritime security awareness.

The study offers the following important strategic shifts to prevent regret in 2028. Foremost, the Department of Defense (DOD) must increase its emphasis on deterrence and homeland defense through credible offensive capabilities. The Department also needs to shift from primarily kinetic, high-cost ways of war to more non-kinetic methods in order to reverse the effectiveness of asymmetric counters from our adversaries. While these may seem to be dramatic departures from more traditional DOD missions, the study determined that staying on the current course will result in deep regret in 2028 and beyond. Further, the capacity to make these shifts is well within the capabilities of the Department and is already underway in many areas.

This report is in some ways a companion piece to the recent DSB report on *Technology Strategy*. That report took a "quick look" at ten selected technologies, capabilities, systems, and missions with relevance to the Office of the Under Secretary of Defense for Research and Engineering. These areas were (1) cybersecurity

technology, (2) microelectronics technology, (3) quantum science and computing, (4) machine learning and artificial intelligence; (5) directed energy; (6) command, control, and communications, (7) space offense and defense; (8) hypersonic offense and defense; (9) missile defense; and (10) nuclear deterrence. While there are some areas of overlap, these two reports together cover a large fraction of important defense research and engineering.

While these two studies have provided "quick looks," the DSB has followed these studies with a number of task forces charged with taking a deeper dive into many areas. Currently underway are studies on Biology, Strengthening Counterintelligence Capabilities Against the 'Insider' Threat, and Counter Autonomy; as well as the 2019 Summer Study on the Future of U.S. Military Superiority, a broader study looking at both superiority undersea and superiority in the information environment. Task forces on several other topics are planned to start later in 2019, including homeland defense against ballistic and cruise missiles, resilience of the U.S. electrical grid, resilience of the U.S. defense industrial base, and resilience of U.S. positioning, navigation, and timing.

While we look forward to learning the findings and recommendations of these ongoing and planned task forces, we find the discussion and recommendations in this report compelling. We endorse the recommendations detailed in this report and urge the Department to move quickly towards their adoption.

Dr. Craig Fields
Co-Chair

Dr. Eric Evans
Co-Chair

Executive Summary

The Defense Science Board has studied many technologies, capabilities, and missions over more than 60 years of service to the DOD, often focusing on how potential adversaries could achieve Strategic Surprise. Accordingly, this report provides a summary of both new and previously visited topics that bring us up to the present day. Recent surveys in this vein include the 2018 study on Technology Strategy and the 2014 study on Strategic Surprise. Both of these studies provide "quick looks" at key technology and capability areas, and actions recommended to the Department today, that if not taken, would lead to potential regrets in 10 years.

Topics studied have included defense against threats from ballistic and cruise missiles, nuclear proliferation, insider threats, cyber threats, and autonomous weapons. The Board has also studied superiority in the undersea, space, cyber, and the information environment. Recent studies have focused on resiliency of command, control, and communications; positioning, navigation, and timing; logistics, and U.S. electrical grid. And finally, the Board has been chartered since its beginning to study technology trends, including in recent years such areas as biology, microelectronics, quantum science, and machine learning.

This study has focused on areas that—if neglected—would cause significant vulnerabilities and risk for future U.S. national security. Compelling investments have been identified in areas including homeland defense, cybersecurity, gray zone warfare, and emerging technologies such as counter-autonomy and biology. The Board also offers overall summary conclusions based on trends observed in this study and in other recently completed and on-going studies.

A Shift in Defense Missions

Many of the defense missions considered in this study extend beyond DOD's "traditional" missions to deter conventional and nuclear armed conflicts with adversary states and in the event deterrence fails, to win our nation's wars. Other national security missions—including homeland defense, operations in the gray zone, supporting the industrial base—are often treated to be "lesser-included cases" of the traditional DOD missions, or as "other duties as assigned."

As the 2018 National Defense Strategy makes clear, the homeland is no longer a sanctuary. This signals a fundamental shift in thinking about national security and the potential expansion of DOD's mission. Half a century ago, the public reasonably and automatically equated responsibility for all of national security with the DOD, embodied by the Military Services and supported by the Intelligence Community. Today, national security also depends strongly on the Department of Homeland Security and other government entities. Thus efforts in DOD and the Department of Homeland Security (DHS) are also substantially entwined both with each other and with the whole of government: the Department of the Treasury; the State Department; many other federal, state, and local organs of government; and partnerships with allies. Coordination of multiple agencies and organizations remains a serious challenge as organizational authorities overlap and capabilities do not always align with authorities. Adding to the complexity is the overlapping jurisdiction of Congressional Committees. Not surprisingly, inter-agency coordination and decision timelines are labored and incompatible with the velocity of emerging technologies as well as current and future threats.

For historical reasons, there is generally much less emphasis within the DOD on protecting the homeland as compared to protecting American interests abroad. The allocation of resources—monetary, physical, and senior leadership attention—is focused on protecting America's interests abroad, most often by maintaining substantial forward deployed military forces. This is partly the result of a traditional mindset that has long viewed the homeland as a sanctuary, protected by two oceans and friendly states on our borders. Moreover, post-Cold War defense planning focused on rogue regional regimes that lacked the means to directly attack the United States. Today, the threat picture has dramatically changed. The United States faces advanced state competitors, in China and Russia, with the means to carry out very damaging kinetic and non-kinetic attacks on U.S. infrastructure. These could range from attacks on undersea communications cables using remote underwater vehicles to cyber-attacks across a range of largely soft targets. Moreover, the weaponization of cyber capabilities and increasing digital connectivity means less capable adversaries and even non-state actors can inflict often non-attributable damage to American civilian and military infrastructure.

In short, emerging technologies are changing the character of warfare such that the traditional delineation between the front-line combat zone and secure rear areas no longer applies. Likewise, the notion of the homeland as a sanctuary should be discarded and replaced with an assumption that in the event of conflict, great power competitors such as China and Russia, will seek to cripple U.S. military command and control, the ability to assemble and transport forces overseas, and the ability of the industrial base to support military operations. A combination of both civilian and military dependence on computer networks and advanced cyber weapons means these attacks could be carried out at a covert level that poses real challenges in terms of retaliation and escalation.

It is increasingly clear the two domains—protecting U.S. interests at home and abroad—are inexorably linked. While there is no strict division between these two overarching missions, the balance of attention across the government between them deserves analysis. Prioritization does not imply a strict sequential application of resources, but it does inform application of resources. Both protecting Americans at home and protecting Americans abroad often require the same technologies and capabilities.

The changing character of warfare is driving an expansion of potential threats to U.S. interests at home and abroad. This study identified four major themes that contribute to this situation.

1 Shifting and Expanding Attack Surfaces against the U.S.

Many of the areas described in this study need attention because of the expanding and diversifying attack surfaces that U.S. adversaries can now exploit. DOD has not yet caught up to the impact of dramatically advancing technologies that are driving changes in the very character of war along with what is a rapidly changing threat landscape. For example, attribution methods and sufficiently clear declaratory policy for biological threats is lacking; and many legacy systems retain vulnerabilities to strategic cyber attack and the U.S. remains tentative in using the offensive capabilities on hand. The U.S. has traditionally assumed the mission to defend everything, everywhere—around the globe, undersea, and in outer space—and today increasingly in cyber space, in the gray zone and in the information environment. Continuing to expand the current U.S. defense posture is increasingly expensive and will not guarantee protection against these

vulnerabilities, nor will this approach always be able to counter the variety of new threats constantly emerging. This current trajectory has increased the asymmetry between the increasing cost of U.S. defenses and the decreasing cost to adversaries to counter those defenses and needs to be reversed.

2 Breaking from the Past

Sunk costs, bureaucratic inertia, or tradition have had a large impact on impeding the rapid fielding at scale of new capabilities for emerging national security challenges. Most current U.S. capabilities and investments remain platform-centric and are highly centralized and hence highly vulnerable: ships, planes, tanks, satellites and missiles that can be readily targeted by a range of new threat systems and tactics employed by U.S. adversaries. As more than 70 percent of the lifecycle weapons costs are in their sustainment, combined with the practice of maintaining such systems over many decades, makes dramatic change difficult. This becomes more challenging with the increasing concern for the rising cost of medical and retirement benefits for military personnel. For these reasons, adversaries can pose significant threats at a fraction of the U.S. defense budget.

3 Embracing Non-traditional Missions

In several instances, U.S. defense policy has arguably neglected a problem. The most glaring example is the gray zone—the emerging profile for war that never escalates to armed combat and incorporates economic, information, espionage, and influence operations. The U.S. is only beginning to systematically counter actions below the threshold of use of major force. Another example of a problem neglected, as evidenced by the experience in Iraq and Afghanistan, is stabilization, reconstruction, and peacekeeping and countering the inevitably accompanying counter-insurgency. Too often, the U.S. finds itself unprepared for these missions. These cases require policy decisions and the will to employ or tweak current capabilities rather than the development of entire suites of new capabilities.

4 Sharing the Responsibility for National Security

It has become increasingly clear that while DOD remains the first line of national defense, this is primarily because it is the only Department with operational capability at scale. Almost every mission, however, will require coordination with other cabinet departments. Homeland defense is most obviously a partnership with DHS, but also requires a high degree of involvement with local and state agencies. The diplomacy mission is coordinated with the State Department, along with the Department of the Treasury, Department of Commerce, and the U.S. Trade Representative which all play a role in deterrence. All work on nuclear weapons and deterrence is coordinated with the Department of Energy, and many more agencies are involved in post-conflict stabilization efforts.

Strategic Shifts are Needed

A number of strategic shifts have been identified for the DOD to address this challenge. These shifts are recommended to the Secretary of Defense, the Joint Staff, and the Military Services to modernize U.S. planning and investment approaches, with the goal to reverse the unfavorable cost trends and increase the effectiveness of DOD's efforts. A number of these are in the realm of operations and investments designed to shape our competitor's strategic calculus in ways that

advantage the U.S., something DOD did routinely during the Cold War, and that will require exercising strategic muscles that have been allowed to atrophy in the intervening decades.

Implementing this change will require a two-pronged approach. First, identifying existing and planned capabilities that, while meeting "validated requirements," will only increase the cost of defense systems without protecting against low-cost attacks. Second, to adequately resource the development of new capabilities and new concepts as part of a sustained strategic competition to reverse this unfavorable asymmetry and create operational dilemmas for competitors and adversaries.

A critical finding in the report is that credible deterrence is almost always more cost effective than defense, and a variety of disruptive offensive capabilities were identified that can provide credible deterrence levels. As much as new capabilities, devising new operational concepts, new ways of warfighting, are a critical part of reversing an unfavorable cost equation. Our competitors and adversaries have thoroughly studied the American way of war and developed a suite of capabilities to defeat the military's preferred way of fighting. The DOD must expend the intellectual energy to develop innovative operational concepts that depart from the military's prepared s script and present our adversaries with unanticipated offensive moves that seize and maintain initiative and keep them on their heels reacting to our actions.

Shifting away from primarily kinetic ways of war was identified as another approach to focus on asymmetric counter value actions against adversaries. Emphasizing non-kinetic means— such as cyber offense and defense, biology and related technologies, improving the resiliency of U.S. positioning, navigation and timing, defeating large numbers of autonomous systems, and electronic warfare—can be less escalatory and more cost effective to defend the U.S. both at home and abroad.

Another key aspect of deterrence is the utilization of reversible and graded actions that allow de-escalation and aid stabilization. Superiority in the information environment, can effectively avoid any actions that could force adversary leadership to radically escalate in response to population unrest.

Finally, an important strategy to reverse the current asymmetry is to increase the focus on DOD's role in homeland defense. This includes a thorough look at options for defense against ballistic and cruise missiles in the continental United States (CONUS) and DOD's role in resilience of the U.S. electrical grid and maritime security. The resilience of the U.S. defense industrial base and defense against insider threats are additional aspects of homeland security that deserve renewed attention to prevent serious regrets in 2028.

These strategic shifts are proposed guidance of any analysis of alternative, operating plan, or investment strategy across DOD. They should together enable DOD to reverse the adversaries' asymmetric advantages and to reduce the increasingly disproportionate costs to defend our interests at home and abroad.

Study Membership

Study Chairs

Dr. Craig Fields	Private Consultant
Dr. Eric Evans	MIT Lincoln Laboratory

Executive Secretaries

Mr. Kevin Doxey	Defense Science Board

Members

Dr. Amy Alving	Private Consultant
Dr. Michael Anastasio	Private Consultant
Mr. Michael Bayer	Private Consultant
Mr. Frank Cappuccio	Private Consultant
Mr. James Carlini	Leidos
Gen Michael Carns, USAF (Ret.)	Private Consultant
Dr. Arup Chakraborty	Massachusetts Institute of Technology (MIT)
Dr. David Chu	Institute for Defense Analysis (IDA)
Dr. Victoria Coleman	Wikimedia Foundation
Dr. Ruth David	Private Consultant
Mr. Christopher Day	Cyxtera
Mr. William Delaney	Private
Consultant ADM William Fallon, USN (Ret.)	Private
Consultant Dr. Kaigham (Ken) J. Gabriel	Draper
Laboratory	
Mr. James Gosler	JHU Applied Physics Laboratory
Mr. Al Grasso	Private Consultant
Mr. Page Hoeper	Private Consultant
Dr. Miriam John	Private Consultant
Dr. Anita Jones	University of Virginia
Dr. Paul Kaminski	Technovation, Inc
Dr. Ronald Kerber	Advanced Technology International
Gen. Paul Kern, USA (Ret.)	The Cohen Group
Dr. William LaPlante	MITRE Corporation
Dr. John Manferdelli	Northeastern University
Dr. Joe Markowitz	Private Consultant
Dr. Mark Maybury	Stanley Black and Decker
Dr. James Miller	Private Consultant
Dr. Judith Miller	Private Consultant

Mr. Robert Nesbit	Private Consultant
Dr. Paul Nielsen	CMU Software Engineering Institute (SEI)
Mr. Michael Rich	RAND Corporation
Mr. Mark Russell	Raytheon
Dr. William Schneider	International Planning Services, Inc.
Dr. Ralph Semmel	JHU Applied Physics Laboratory
Mr. James Shields	Private Consultant
Mr. Robert Stein	Private
Consultant VADM Edward Straw, USN, (Ret.)	Osprey
Venture Partners	
Dr. James Tegnelia	University of New Mexico
Mr. David Van Buren	L3
Mr. Vincent Vitto	Private Consultant
Mr. Lewis Von Thaer	Battelle
Dr. David Whelan	University of California at San Diego
Dr. Robert Wisnieff	IBM

DSB Staff

LtCol Milo Hyde, USAF	Defense Science Board
Mr. Edward Gliot	Defense Science Board
Mr. David Moreau	Defense Science Board

Staff

Ms. Elizabeth Armistead	Strategic Analysis, Inc.
Ms. Hannah Schmidt	Strategic Analysis, Inc.
Mr. Kevin Gates	Strategic Analysis, Inc.
Ms. Ashlee Gilligan	Strategic Analysis, Inc.
Mr. Marcus Hawkins	Strategic Analysis, Inc.
Mr. Brian Keller	Strategic Analysis, Inc.
Dr. Toni Marechaux	Strategic Analysis, Inc.
Ms. Christine McCorkle	Strategic Analysis, Inc.
Dr. Adrian Smith	Strategic Analysis, Inc.
Ms. Melissa Smittle	Strategic Analysis, Inc.
Mr. Ted Stump	Strategic Analysis, Inc.
Mr. Daniel Young	Strategic Analysis, Inc.

Terms of Reference

THE UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH
AND ENGINEERING

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference - Defense Science Board 2018 Summer Study on Strategic Surprise

The objective of the 2018 Defense Science Board (DSB) Summer Study is to consider what potential technical capabilities may not be sufficiently acted upon by the Department of Defense (DoD) in the decade to come, that will lead to U.S. regrets in 2028 and, in broad terms, what those actions might be.

Considerations for each recommended emerging technical capability should include: maturation of science and technology; the development of new weapons and weapon concepts (including weapons of mass destruction); the emergence of new operational concepts and rules of engagement; different potential adversaries and different kinds of potential adversaries; changing alliances among potential adversaries and changing relationships between the United States and its allies; broad global trends such as demographic shifts, geopolitical changes, resource constraints or climate change; evolving priorities for national security objectives; and, U.S. foreign policy goals.

This summer study will be sponsored by me as the Under Secretary of Defense for Research and Engineering (USD(R&E)). I am authorized to act upon the advice and recommendations of the DSB. The current DSB Chairman, Dr. Craig Fields, and Vice-Chairman, Dr. Eric Evans, will serve as co-chairmen of this board-level study. Mr. Edward Gliot, acting Executive Director, will serve as the Executive Secretary and DSB Secretariat Representative.

The study members are granted access to those DoD officials and data necessary for the appropriate conduct of their study. The USD(R&E) will serve as the DoD decision-maker for the matter under consideration and will coordinate decision-making as appropriate with other stakeholders identified by the study's findings and recommendations.

The study will operate in accordance with the provisions of Public Law 92-463, the "Federal Advisory Committee Act," and DoD Directive 5105.04, "DoD Federal Advisory Committee Management Program." It is not anticipated that this study will need to go into any "particular matters" within the meaning of title 18, United States Code, section 208, nor will it cause any member to be placed in the position of action as a procurement official.

Michael D. Griffin 4/20/2018