DEPARTMENT OF DEFENSE
DEFENSE SCIENCE BOARD

TASK FORCE ON

DETERRING, PREVENTING, AND RESPONDING TO THE THREAT OR USE OF WEAPONS OF MASS DESTRUCTION

EXECUTIVE SUMMARY

May 2018

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
WASHINGTON, D.C. 20301-3140

DEFENSE SCIENCE BOARD

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

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

SUBJECT: Final Report of the Defense Science Board (DSB) Task Force on Deterring, Preventing, and Responding to the Threat or Use of Weapons of Mass Destruction

I am pleased to forward the final report of the DSB Task Force on Deterring, Preventing, and Responding to the Threat or Use of Weapons of Mass Destruction, chaired by Dr. Miriam John and Dr. William Schneider.

The Task Force divided its findings into three specific areas – Early Warning, Chemical and Biological Threats, and Nuclear Threats. First, the Task Force found that timely warning of proliferation significantly expands options for deterrence. Augmenting traditional intelligence sources with open sources shows promise for early proliferation detection. Second, chemical and biological threats have historically been addressed through protection or response; the Task Force recommends these threats can and should be addressed more broadly in a deterrence context. Defense-in-depth, from warning through attribution and requisite retaliation, is feasible, and more importantly, critical to addressing emerging threats. Finally, nuclear deterrence requires relearning much of what has been forgotten with regards to the principles, but applying them with new tools and unprecedented integration. That integration should leverage conventional, nuclear, and non-kinetic capabilities coupled with messaging and demonstrated operational flexibility to strengthen deterrence and assurance, better manage escalation risks, and widen the options available to leadership.

I concur with the Committee's conclusions and recommend you forward the report to the Secretary of Defense.

Craig Fields
Chairman, DSB

THIS PAGE LEFT INTENTIONALLY BLANK

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

DEFENSE SCIENCE
BOARD

MEMORANDUM TO THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Executive Summary of the Final Report of the Defense Science Board (DSB) Task Force on Deterring, Preventing, and Responding to the Threat or Use of Weapons of Mass Destruction: Chemical and Biological Threats

Attached is Executive Summary of the final, multi-volume report of the Defense Science Board Task Force on Deterring, Preventing, and Responding to the Threat or Use of Weapons of Mass Destruction (WMD). The Task Force was charged with identifying ways in which deterrence can evolve given a changing security environment, and should deterrence alone prove inadequate, identifying additional ways to prevent and respond to an attack. Under the Terms of Reference, it was stipulated the Task Force should address the following questions:

- What capabilities are available for early detection of WMD research, development and acquisition?
- What technology advances are necessary to deter or prevent further progress by proliferants once detected?
- How far can such advances and others that are yet to be fielded go in deterring further proliferation or WMD use?
- Will declared policies and capabilities remain sufficiently credible?

The Task Force organized its findings and recommendations for WMD deterrence into three areas: Early Warning, Chemical and Biological Threats, and Nuclear Threats. First, warning of proliferation as early as possible significantly expands options for deterrence. Augmenting traditional intelligence sources with open sources shows promise for early proliferation detection. Second, chemical and biological threats, historically addressed through protection or response, can and should be addressed more broadly in a deterrence context. Defense-in-depth, defined as layered defensive elements which are self-reinforcing, from warning through attribution and requisite retaliation, is feasible and critical for addressing emerging threats. Finally, nuclear deterrence today requires applying new tools to the traditional principles of nuclear deterrence together with unprecedented integration of nuclear, kinetic and non-kinetic capabilities.

Separate volumes cover each of the three areas. This Executive Summary provides a compilation of the separate executive summaries from each of those volumes.

Dr. Miriam John
Co-Chair

Dr. William Schneider
Co-Chair

THIS PAGE LEFT INTENTIONALLY BLANK

DSB Task Force on DETERRING, Preventing, and Responding to the Threat or Use of Weapons of Mass Destruction

Executive Summaries

Table of Contents

THIS PAGE LEFT INTENTIONALLY BLANK

Overview

The Defense Science Board Task Force on Deterring, Preventing and Responding to the Threat or Use of Weapons of Mass Destruction was given a broad charter, found in the Terms of Reference of Appendix A. In undertaking its information gathering and assessing the most important issues for leadership attention, the Task Force decided that its findings and recommendations were best presented in three major areas, in part because the principal audiences for each differed and in part because the nature of what should be done with each is quite different. The three areas are:

Early Warning. As the Task Force defined it, early warning refers to persistent monitoring for nascent or emerging information at the earliest stages of the potential development of a threat and throughout the stages of evolution of that threat. The timescale involved depends on threat chains of events. With respect to WMD, "early" includes detecting intent that could be evident years in advance of capability, and thus years ahead of the realization of the threat. The importance of early warning rests on the premise that the earlier the warning, the more options available to U.S. decision makers to prevent further progress in developing or proliferating a WMD capability.

Improvements in early warning, as viewed by the Task Force, can be made with the application of emerging technologies in "big data" management and data analytics. Responsibilities fall across a number of organizations within the intelligence community and with key agencies, such as the Defense Threat Reduction Agency (DTRA), within DoD. The Task Force recognized that it would take all of the players working together for success, and debated implementation options for such an interagency effort. To that end, the Task Force recommends an executive agent be assigned jointly by the Director of National Intelligence and Secretary of Defense to replace the current interagency committee approach that functions to coordinate without the authority to plan and integrate efforts.

Chemical and Biological Threats. The level of attention to either chemical or biological weapons (CB) defense rises and falls with events. As a result, progress has been limited and priorities frequently reset over the course of the last two decades. At the same time, technical advances have continued to make agents and delivery means ever more accessible to threat actors across the spectrum from nation states to lone wolves, who can achieve some level of capability with limited investments and by "hiding in plain sight" their acquisition and deployment efforts among otherwise legitimate activities.

Having foregone response-in-kind as a factor in dealing with the CB threat, the United States has relied on defense, principally based on protection and response to specified threat agents, as its strategy. The Task Force, prompted by the promise of technologies to support early warning as noted above, by the improving cost effectiveness of detection and diagnostics, and by new approaches for achieving readiness for medical preparedness and countermeasures, concluded that a more robust defense-in-depth strategy was not only possible but critical to addressing the spectrum of agents we might face in the future. By defense-in-depth the Task Force means a

system of integrated, cooperating elements – from pre-attack to post-attack – instead of stand-alone components. None need work perfectly, but shortfalls in one are compensated by strengths in another. Collectively the system creates sufficient uncertainty that an attack will succeed such that the perpetrator is deterred from attacking at all.

The Task Force went into some detail to delineate the potential elements of such a strategy to illustrate what it might look like. It is recommended that the key offices responsible in DoD undertake their own assessment, posit an integrated strategy, test it against a range of scenarios, and implement key development and operational steps that result. Sustainment is key, however, so that attention must be given to a steady effort undertaken by career professionals, not one that is revectored based on episodic events as has too often occurred in the past.

Responding to Nuclear Threats. Nuclear weapons have again become a major element of international security affairs, but since the end of the Cold War significant nuclear threat asymmetries have emerged. Combined with capabilities in new threat domains (e.g., cyber, counter-space, precision strike), adversaries are developing asymmetric strategies and operational concepts that pose a risk to long-standing U.S. goals for regional security, extended deterrence, strategic stability, and nonproliferation. Not only must the United States continue to deter major nuclear war, but once again must face the challenge of deterring, and if necessary fighting, a regional conflict with one or more nuclear-armed adversaries.

These challenges require intensified effort along these three interrelated lines:

- A more integrated concept for strategic deterrence that leverages conventional, nuclear and non-kinetic capabilities coupled with messaging and demonstrated operational flexibility to strengthen deterrence and assurance, better manage escalation risks, and widen the options available to leadership;
- Integration of early warning in defense planning conducted continuously as a campaign to provide enduring insight into adversaries' intent, capabilities, and plans in order to maximize opportunities to prevent, deter, and/or defeat;
- A more adaptive nuclear enterprise able to hedge against future threat developments through exploratory and advanced research, development and prototyping, and a modernized and agile production approach.

Specific recommendations are directed to DoD, the Department of Energy and the intelligence community.

For each of the three areas above, a stand-alone report has been written.[1] What follows here are the Executive Summaries reproduced from each of the stand-alone reports, so that the reader can quickly get a view of the scope and results of the Task Force's work.

[1] The Task Force on Deterring, Preventing, and Responding to the Threat or Use of Weapons of Mass Destruction, Volume I: Early Warning, Volume II: Chemical and Biological Threats, and Volume III: Responding to Nuclear Threats.

Early Warning

The potential threats posed by weapons of mass destruction (WMD) to both military forces and civilians are serious and growing. Across the spectrum from preventing to responding to such threats, the earlier the warning, the more options for countering them. The Task Force found, however, that capabilities to do so (i.e., detecting proliferation or use much earlier than our experience to date) lag what is both needed and doable. The key challenge lies in the combined exploitation of all relevant information sources, especially open source information (OSI), to maximize opportunities for early warning with the potential to discover intent well before acquisition. Multidisciplinary applications of processing and analysis of big data at scale have enabled significant strides in early threat detection in other domains, more often in tactical and/or single intelligence (INT) applications. The dangers posed by WMD, when considered in the context of the demonstrated successes of early warning in other applications and the rapid technical advances being made in the relevant tools, should provide all the motivation needed to significantly improve our abilities to detect and, therefore, deter those actors who are seeking to acquire and use WMD.

The challenges for WMD early warning are both technical and organizational. Technically, early warning for WMD intent requires persistent, 24/7 data analysis in near real-time using multi-INT data collection at global scales over months to years. The data challenges surpass those of counterterrorism (CT) and include collection, storage, processing, exploitation, visualization, and decision making. Architectures must be tailored to specific nuclear, chemical, and biological domains, but should be constructed to allow analytic teams to share and compare findings and techniques. These capabilities and "truth data sets" to verify and to validate algorithm effectiveness are limited to non-existent, and they must be developed to have confidence in analytic results.

There is significant promise in the comprehensiveness and exploitation of OSI. The growing volume, velocity, variety, and value of OSI can provide rich detail on people, organizations, relationships, biometrics, geography, and transactions, whether targeted for collection or not. The platforms, data, and tools for exploiting OSI are already here, available for exploitation, and growing daily. Because our adversaries, antagonists, and their supporters are dependent on open source communication channels, OSI can potentially provide answers to many different classes of intelligence problems. OSI can assist targeting and battle damage assessment (BDA), and can provide access to anti-access area denial (A2AD) environments, as even the most closed geographies and groups must procure, transit, and bank. Finally, OSI has the added benefit of being shareable with allies and other mission partners as long as the sources and methods are protected. When done right, the community should be able to cue across classifications in a dynamic feedback loop.

Realizing the technical potential of OSI integrated with classified sources, however, will require cross-community integration analogous to what has happened in the CT mission. Organizationally, WMD early warning currently depends on a “coalition of the willing.” The long-term nature of WMD proliferation is vulnerable to the urgent re-tasking of resources to short-horizon problems.

A dedicated, INT-agnostic analyst community with a rich toolkit of models, data, and analytics is needed, but does not yet exist. Progress at any significant level will require a transparent and persistent level of interagency engagement across the government.

Given the technical and organizational issues and opportunities identified by the Task Force, the following recommendations are provided for achieving a major step forward. We can and must do much better against WMD threats in a world brimming over with "open secrets."

Recommendations

EW-1. Realizing the Potential of OSI. The **Director of National Intelligence (DNI)** should direct the **National Counterproliferation Center (NCPC)** to lead in establishing a collaborative virtual laboratory that brings together analysts, data, operators, planners, technologists, and subject matter experts (SMEs) to address WMD problems to realize the full potential of emerging OSI for detecting and monitoring illicit WMD activities.

EW-2. Significant Role of Tipping and Cueing. In parallel with the virtual laboratory, the NCPC should bring together **intelligence community (IC) partners** to explore means by which open and classified sources can cross-cue each other to improve the performance of WMD early warning. This effort should include the creation of data sets and early warning threat models to support such tipping and cueing. The models should explicitly incorporate tactics, techniques, and procedures (TTPs) and roles of tipping and cueing so exploitation algorithms can be developed and more fully automated.

EW-3. Enabling Open Architectures. The **Intelligence Advanced Research Projects Activity (IARPA)** and the **Defense Advanced Research Projects Agency (DARPA)** should develop architectures that support open and classified information to co-mingle and perform common functions (e.g., logistical path detection and covert financing) across all WMD domains while allowing deep dives into domain specific challenges (e.g., nuclear forensics and disease mapping).

EW-4. Organizing a Multi-Agency Approach. The **National Security Council (NSC)** should expand existing policies to address detection and early warning for all WMD domains.

The **DNI**, the **Secretary of Defense (SECDEF)**, and the **Secretary of Energy** should appoint an executive agent (EA), provide the EA with seed money, and establish either a Joint Interagency Task Force (JIATF)-type model or integrated planning team (IPT) model to provide global early warning that extends beyond National Intelligence Production Framework (NIPF) targets. The NCPC and the U.S. Special Operations Command (SOCOM) – with its countering weapons of mass destruction (CWMD) mission responsibilities – should be considered as leading EA candidates.

The DNI should establish consistent policies related to OSI to mitigate any risks as well as duplicative and/or suboptimal efforts.

EW-5. Building the Workforce for Early Warning. The **Office of the DNI (ODNI)** should lead a cultural shift to transform IC and DoD early warning workforces to promote cross-cutting, multi-INT analysis and decision making, focusing on overcoming non-multi-INT stovepipe systems and cultures.

Chemical and Biological Threats

The ability of the Department of Defense (DoD) to deter and defend against chemical or biological attacks has not been assessed in the context of the current threat environment or recent developments and technical trends that will impact the future. Preparedness has been dominated by a focus on dangerous but well-understood Cold War threats. All the while, chemical weapons (CW) and biological weapons (BW) have continued to be developed elsewhere. The most visible example of CW concerns is the use of chlorine, a commercial chemical, by the Syrian government against its own citizens in violation of the Chemical Weapons Convention (CWC).[2,3] The familiar BW threats still exist; however, with the rapid advances in synthetic biology, there is potential for fundamentally new classes of biological threats, which are nearly impossible to predict at this point. Simply adapting existing strategies to new technologies will be insufficient. The historic emphasis on protecting the warfighter by setting requirements for "point" solutions to the scenario or agent at hand must give way to a broader end-to-end approach for which deterrence of an attack should be the goal.

Deterring Chemical or Biological Attacks through Defense-in-depth

Because the United States has foregone response-in-kind in the chemical or biological domains and because pre-attack detection and interdiction are difficult, the primary tenet of deterrence – to hold at risk what the adversary holds dear by guaranteed response-in-kind – needs to be reassessed in the context of broader objectives of the attacker. The Task Force assessed that deterrence could be best accomplished by making an adversary choose a course of action that is most favorable to us. As with nuclear deterrence, a CW and BW deterrence "victory" is the absence of an attack, not an attack that is successfully defeated. In contrast to nuclear deterrence, however, deterrence of CW or BW must be based on a calculus of ***harm (to us) avoided***, rather than ***harm (to them) inflicted***. The Task Force came to the conclusion that deterrence through a defense-in-depth strategy was the best, if not only, plausible approach, provided the strategy includes a comprehensive set of elements from pre- to post-attack. A robust, integrated defense-in-depth strategy would provide visible and powerful collective deterrence, make adversaries uncertain an attack will succeed, suggest there will be successful attribution and painful retribution, and leave elements of U.S. capabilities ambiguous.

Defense-in-depth is designed to be a system, built on integrated, cooperating elements rather than a collection of stand-alone programs. The strengths of one element are intended to

[2] White House Office of the Press Secretary, "Government Assessment of the Syrian Government's Use of Chemical Weapons on August 21, 2013," August 30, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/08/30/government-assessment-syrian-government-s-use-chemical-weapons-august-21.

[3] Organisation for the Prohibition of Chemical Weapons, "OPCW Fact-Finding Mission Confirms Use of Chemical Weapons in Khan Shaykhun on 4 April 2017," June 30, 2017, https://www.opcw.org/news/article/opcw-fact-finding-mission-confirms-use-of-chemical-weapons-in-khan-shaykhun-on-4-april-2017/.

compensate for the weaknesses in others. It is designed to produce uncertainty in outcomes of attacks in the minds of adversaries. Through the comprehensiveness and overlapping of elements, it moves toward equalizing "us" with "them." They have many options for attack; we have many options for defense and response. They will often not have the technical sophistication and/or resources required to analyze and understand our components and capabilities to a degree that provides confidence in the success of attacking.

As a system, defense-in-depth allows us to adapt our response to what we encounter. By integrating the components into a system, we get, or can require, coordination and cooperation of components. Collecting components into a larger strategy brings better visibility to the effort, as well as opportunities for messaging, both factually and through denial and deception.

From an organizational and administrative perspective, CW and BW have often been lumped together as a single class of threat, arguably at some disservice in developing defenses against each. At a high level, chemical and biological weapons have similarities (e.g., low barriers for entry and are almost always intended to kill or incapacitate people, not destroy structures or other weapon systems). They differ, however, in important and specific ways. While both have continued to evolve, they have done so as separate classes of threats, in large part because their effects differ, as do the technologies to counter them. The prospects for further development of the threat differ as well, with the rapid advances in bioscience and biotechnology posing a higher risk for surprise. ***The nature of the similarities and differences between CW and BW, therefore, argues a defense-in-depth strategy can be based on common elements, but implementation of the strategy should be different for CW and BW***.

Figure ES-1 presents the elements and example components for a defense-in-depth strategy.

Defense-in-depth Element	Example Components
Prevention	• International diplomacy and controls – International cooperation (e.g., updated conventions, involvement of public health groups, shared intelligence) • Science diplomacy (e.g., lab-to-lab) • Materials security
Active Awareness	• Early warning • Open source exploitation • Red teaming • Modeling and simulation
Messaging	• Exercises and demonstrations • Publications and conferences • Denial and deception
Interdiction and Neutralization	• Pre-attack interdiction • Weapon disablement or neutralization
Mitigation and Recovery	• Preparedness (i.e., planning, training, and practice) • Selective "hardening" (e.g., "smart" buildings) • Attack detection and characterization • Medical and non-medical countermeasures • Restoration and recovery
Attribution and Response	• Forensics • Retribution by other means (e.g., financial, conventional weapons)
Strong Tech Base and Adaptive Management	• Integration of multiple skills (i.e., from intelligence to chemical decon) • Enhanced career opportunities • Engagement with pharmaceutical companies and universities • Demonstration of readiness and learning opportunities by responding to natural disasters and outbreaks globally

Figure ES-1. Elements of defense-in-depth

With the above elements and components in mind, **Figure ES-2** summarizes the Task Force's assessment of general requirements and selected actions against a range of possible attacks.

Type of Attack	Requirements	Exemplary Actions
1. Isolated Terrorist in the Homeland	• Early intelligence supporting interdiction and prevention • Control of public reaction • Casualty care • Restoration of function • When and where the DoD's role occurs	• Gaming, coordination, and policy • Training and exercising • Rapid diagnostics and treatment • Technology to facilitate cleanup
2. Against U.S. Military Operations Using World War II and Cold War Threat Technologies	• Ability to operate under competent attack • Casualty care • Restoration of function	• Realistic testing and gaming against nation state red teams • Improved protective systems • Preparedness (i.e., stockpiling vaccines and countermeasures, protective systems) • Integrated capabilities to respond to chemical and biological attacks • Emphasis on intelligence and supporting technology
3. Against U.S. Military Operations Using Current Technologies	• Protective technologies • New types of casualties • New delivery systems (e.g. drones, precision weapons)	• Same as above (#2) • Research and development based on realistic red teaming, and challenge environments • Evaluation of threat characteristics
4. Organized, Prolonged Attacks against the United States (soft targets — e.g., financial assets and populated transportation systems)	• Same as above (#1) • Maintaining public confidence • Preventing severe economic damage • Responsive medical systems • Attribution	• Emphasis on early warning and anticipation • Attribution capabilities
5. Against United States at the Strategic Level; Existential to the United States	• Same as above (#1, #4) • Response at scale (i.e., detection, emergency operations, medical treatments)	• Emphasis on early warning • Technology for accelerated development of vaccines, therapeutics
6. Against U.S. Interests Broadly Using Future Technologies/Unknown Unknowns	• Hedging against surprises, anticipation of tactics, practices	• Emphasis on early warning • Involvement of the DoD with synthetic biology as a strategic threat but also with transformational medical potential

Figure ES-2. Deficiencies and possible remedies for implementing the strategy

As noted in **Figure ES-2**, any mitigation step must take into account the differences between chemical and biological weapons. Those differences are summarized in **Figure ES-3**. Volume II

discusses chemical and biological weapons and particularizes the strategy and deficiencies for each separately.[4]

Aspect	Chemical	Biological
Injury Countermeasures	• Neurological, burn, other pharma countermeasures, agent specific • Palliative or no treatment or physical protection (suits, creams)	• Disease (may be contagious) • Vaccines, anti-infectives, medical supportive care, intelligence critically important
Quantities Required	• Large (military ops) to small (terrorism)	• Small to large
Delivery Systems	• Well-tested dispersal devices; especially effective in contained areas/spaces; accessible to terrorists	• Inhalation of aerosols or in food; more difficult to control dispersion, maintain efficacy of agent
Competence Required to Prepare or Use	• Low (for industrial chemicals) to very high (advanced chemical agents)	• Modest to very high (e.g. short shelf life of agents, narrow size range of inhalable aerosols, effective delivery)
Time from Attack to Symptoms	• Variable (generally minutes to hours)	• Days
Target for Intelligence	• Very difficult and depends on the quantity and agent; easily hidden among legitimate activities	• Very difficult; even more easily hidden or disguised as legitimate activities
Attribution	• Difficult but large quantities for major attack likely to be traceable to a few actors	• Very difficult, for same reasons as intelligence target before an attack
Potential for Future Surprise	• Agents largely known but delivery mechanisms for targeting likely to evolve; new agents possible	• Very probable (e.g., genetic engineering, immunology)
Adversaries Comfort/ Willingness to Use	• Moderate for both state and non-state actors (current active experimentation in uses of Toxic Industrial Chemicals (TIC)); development of some new agents	• Less familiar; more specialized skills needed • Non-state adversaries would likely require expert assistance

Figure ES-3. Comparison of chemical and biological weapons

[4] A classified version of *Volume II Chemical and Biological Threats* is available. To obtain a copy, please contact the DSB office at *osd.pentagon.ousd-atl.mbx.dsb-office2@mail.mil*.

Recommendations for Implementing the Strategy

Volume II of this report discusses chemical and biological weapons more fully and particularizes the strategy and deficiencies for each separately to form the basis for recommendations. The major recommendation of the Task Force is obvious from the above discussion, namely that the Chemical and Biological Defense Program (CBDP), under the leadership of the Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense (ASD(NCB)), should shift its strategy to one based on defense-in-depth. To do so, however, will require time, resources, and a disciplined approach to setting priorities and cultivating expertise. Therefore, The Task Force recommends focusing attention on three areas to ensure the transition from the current state is successful:

- Test the strategy, at the outset and continuously thereafter, in a number of realistic scenarios to establish needs and gaps in capabilities, policies, and operational readiness.
- Aim for much stronger program and operational integration by managing to the technical differences, training, and exercising to the operational differences between CW and BW as well as adapting acquisition practices to the unique requirements for fielding medical countermeasures.
- Value and sustain expertise in both CW and BW defense across the research and development (R&D) to operational spectrum.

TESTING AGAINST SCENARIOS

CB-1. The **ASD(NCB)**, through the **Deputy Assistant Secretary of Defense for Chemical and Biological Defense (DASD(CBD))**, should recast the CBDP as an integrated defense-in-depth program.

- Ensure senior leadership understands the spectrum of threats posed by chemical weapons (CW) and biological weapons (BW), along with opportunities to minimize them.

CB-2. The **CBDP** should develop a defense-in-depth strategy based on identifying the actions required for preventing or mitigating chemical and biological attacks across a broad range of scenarios, followed by an assessment of capability needs and gaps. There should be included steps for communicating the strategy and progress in its implementation to introduce greater uncertainty in the adversary's calculus of success.

- An implementation roadmap should be developed shortly thereafter.
- Periodic updates to the strategy and its implementation should be made based on scenarios adjusted for changes in threat and/or technology.

- A targeted and comprehensive communications plan that addresses policy statements, R&D success stories, exercise visibility, etc., should be integral to execution of the program.

PROGRAM AND OPERATIONAL INTEGRATION

CB-3. The **ASD(NCB)**, through the **DASD(CBD)**, should take steps in the implementation of a defense-in-depth strategy to ensure:

- An independent group (possibly at the Defense Threat Reduction Agency (DTRA)) undertakes realistic red teaming to inform intelligence, operations and training, and testing of countermeasures. For testing, actual agents or well-characterized surrogates are essential.
- The interagency partnership to improve attribution receives the support it needs from the DoD.
- The Office of the Secretary of Defense for Policy (OSD(P)) examines, develops, and promulgates policy regarding other forms of response because retaliation-in-kind to a chemical or biological attack is not possible.
- A medical acquisition expert is appointed as Milestone Decision Authority for medical biodefense products and works closely with the Food and Drug Administration (FDA) to address its specialized processes and flexibility in product approvals.

CB-4. The **CBDP-Joint Science and Technology Office (JSTO)** and the **CBDP-Joint Program Executive Office (JPEO)** should explore new approaches to accelerate advanced medical countermeasures and develop technology for rapid response at scale to unexpected threats and developments.

- Options that should be explored include:
  - a federally funded research and development center (FFRDC) specialized in drug development, regulatory approval, and production;
  - off label investigations;
  - emergency use authorization for Investigational New Drugs (IND); and
  - recruitment of professionals with drug development experience to lead medical countermeasures research, development, and acquisition (RD&A).
- The DoD should focus its technology base (tech base) on what industry and academia cannot/do not do on their own:

- pathogenesis and immunology of threat agents and classes;
- diagnostics for point-of-care, field and definitive care, and identification for disease surveillance;
- discovery and science and technology (S&T) of antivirals and antibacterials; and
- animal modeling and aerosol administration of virulent agents for tech base and advanced development studies.

CB-5. The **CBDP-JSTO** and the **CBDP-JPEO** should develop and implement a set of testing protocols that are more realistic and relevant to both current and emerging threats.

Such an effort should include:

- a "science of surrogates" research activity to better understand the efficacy of agents used in testing as substitutes for live agents when approving protective and diagnostic equipment; and
- independent assessment of testing configurations for their realism in replicating field operations.

CB-6. For biological attacks with agents and delivery means of a more conventional nature, both the **CBDP** and the **Defense Health Agency (DHA)** should revamp preparedness based on a public health model rather than hazardous materials (HAZMAT) response, which is more applicable for CW.

In particular, the DHA should ensure preparedness for a generic, unknown infectious disease/toxin event through experience in supporting responses globally to emerging infectious diseases (EIDs), with objectives in addition to mitigating the crisis at hand that:

- gives SMEs experience with pathogens and outbreaks in areas of increasing strategic importance (e.g., Africa, Southeast Asia, and Latin America);
- tests diagnostics, vaccines, drugs, and barrier nursing/patient care units for infections not endemic to the United States;
- trains DoD medical personnel in concept of operations (CONOPS) for BW events and in real-world medical management;
- uses lessons learned with EID events to inform development and procurements in CBDP;
- exploits the smart/soft power advantage to these engagements so DoD scientists and clinicians can:

- build relationships and capabilities with scientists and health care providers in other countries; and

- gain a sense of global awareness and even early warning signs of threats (e.g., unexpected clusters of disease, vaccination campaigns, scientific papers).

CB-7. The **Military Departments** should educate the forces by first teaching "all-hazards" defense basics in the DoD with an emphasis on preparedness for new types of attacks (e.g., terrorist/insurgents, attacks in densely populated areas).

- "Un-lump" biological from chemical in training programs and train to higher levels of understanding (i.e., traditional mask drills are irrelevant for biological attacks as well as sensors); importance of awareness of early warning; timeliness of response, etc.

- Develop mitigation and response plans to ensure minimum disruption to the mission. For example, a risk-based approach would consider a BW attack less likely in open spaces or against mobile forces (e.g., on the battlefield) and more likely in a city, base, post, or port area. Plans should identify the importance of vigilance for symptoms, appropriate diagnostics, and countermeasures that can be used post-exposure.

CULTIVATING EXPERTISE

CB-8. The **ASD(NCB)**, through the **DASD(CBD)** and in partnership with the **Army** and the **Department of Homeland Security (DHS) Office of Health Affairs (OHA)**, should ensure the retention and cultivation of the SME technical base.

Specific actions that should be taken include:

- providing a level of stable funding to key DoD labs to support longer term research against evolving threats;

- developing partnerships, especially in future biology (largely in U.S. universities, pharma, and biopharma, but also explore internationally) to help deal with technical surprise;

- testing creative ways of improving the technical level of chemical and biological professionals in the Military Departments and the Defense Intelligence Agency (DIA) through aggressive recruiting, dual-use programs (e.g., vaccines, antibiotic resistance), "half-way houses," and incentives;

- supporting career paths for civilian and military scientists and clinicians that foster the understanding of disease and latest technologies over acquisition, with encouragement to seek opportunities to work with the Centers for Disease Control and Prevention (CDC), the World Health Organization (WHO), and international non-governmental organizations (NGOs) during and between outbreaks; and

- most especially, reinvigorating the biodefense medical and bioscience officer corps and/or civilianize medical laboratory leadership.

CB-9. The **DNI** should ensure the IC is correctly staffed and resourced to deal with the difficult problems of CW and BW.

New or expanded avenues of collection and analysis would include:

- exploiting open-source information, since essential information on areas of technical expertise, and operations (i.e., vaccination developments and campaigns, disease outbreaks, hospitalizations) may be most accessible and available there;

- working with universities and pharma/biopharma companies on sensitive subjects, or models for them; and

- following activities of "technical experts," foreign public and university SMEs, suspected government or commercial officials.

Conclusion

The United States is facing a future in which the thresholds for chemical or biological weapons attacks appear to be dropping, in part due to the increasing access to technologies that support both agent synthesis and weaponization, and limited repercussions to recent violations of international norms that range from assassinations to intentional targeting of civilian populations. As a result of the growing and often difficult to predict array of CW or BW threats, this Task Force recommends a shift from protection and response to a more fulsome deterrence strategy based on defense-in-depth. A number of technical, operational, and management actions are recommended. None are likely to be perfect in its execution, but *in toto* and with persistence, their sum can provide uncertainty in the adversary's mind sufficient to deter an attack.

Responding to Nuclear Threats

Deterring the coercive threat or use of nuclear weapons in a world where several adversary states possess nuclear weapons and are incorporating a doctrine of limited use reflects a sharp break from U.S. Cold War experience. As Dr. Brad Roberts, former Deputy Assistant Secretary of Defense for Nuclear and Missile Defense Policy, noted:

> *If the United States faces an adversary that believes that limited nuclear war against the United States can be won, and thus can be fought, then the United States had better have a theory of victory of its own.*[5]

The United States needs to strengthen the credibility of its nuclear deterrent as well as its extended deterrent to U.S. allies and friendly nations to discourage nuclear states from seeking to employ the coercive threat or use of nuclear weapons for diplomatic or military gain. Strengthening the deterrent serves both immediate U.S. security interests and makes a vital contribution to sustaining global non-proliferation norms. These norms are at risk as strategic competitor and adversary states accumulate nuclear weapons and modern delivery systems. Some weapons threaten the United States, but most pose direct threats to U.S. allied and friendly nations.

Since the end of the Cold War, the United States has developed and fielded several important military capabilities for a variety of missions that, for the most part, were deployed unrelated to the nuclear deterrent. These new capabilities, such as long-range precision conventional strike, cyber operations, early warning, counter-space operations, and others, when used in an integrated manner as dimensions of the U.S. deterrent, can affect the confidence a nuclear adversary state and limit its ability to issue coercive threats with nuclear weapons. The credibility of both the nuclear deterrent and the extended deterrent may be enhanced as part of a broader integrated deterrence strategy.

To sustain the nuclear deterrent and the extended deterrent in a multi-polar world with several nuclear states maintaining an adversarial relationship with the United States, these capabilities need to be effectively integrated with existing and planned nuclear capabilities. When so integrated, many of these capabilities can contribute to a capacity to hold adversary nuclear capabilities at risk, and, in doing so, create a wide range of additional options for the President to affect an adversary's capacity and confidence to coercively threaten or use his or her nuclear capability. As several of these capabilities are already fielded, doctrinally implemented, and exercised by both China and Russia, contemporary approaches to the shaping of the deterrent and extended deterrent will need to take these factors into account and maintain strategic stability between the United States and strategic competitor nuclear states. Moreover, as these

[5] Brad Roberts, *The Case for US Nuclear Weapons in the 21st Century* (Palo Alto: Stanford University Press, 2016).

new non-nuclear capabilities have military utility independent of their linkage to Chinese and Russian nuclear capabilities, it is unlikely these capabilities would be abandoned or their use limited in the interests of strategic stability.

An important enabler of this broader approach to sustaining the nuclear deterrent and extended deterrent is embedded in a concept of early warning. The notion of early warning is built on a foundation of the successful fusion and cross-cueing of open source intelligence (OSI) with other intelligence information. The use of fused OSI and other intelligence sources has been successfully employed in monitoring the proliferation of weapons of mass destruction (WMD) as well as a variety of counterterrorism operations. OSI has complementary characteristics to other intelligence sources and is persistent where other intelligence sources are sometimes episodic in their coverage of adversary targets. OSI is universal in that every nation state and subnational entity emits information by electronic or other means that can be collected and processed, providing knowledge and insight.

Other intelligence sources depend on extraordinarily effective collection and processing technologies that are often fragile if exposed and subject to a loss of access if discovered by an adversary. OSI cannot be blocked, even though it can be spoofed and otherwise manipulated. The risk can be mitigated by advanced analytic techniques. While some intelligence sources must be specifically tasked for a collection mission, OSI cannot be tasked; the information is simply available to be collected. The exploitation of the technologies of big data analysis permits ingesting and processing heretofore unimaginable quantities of data generated by modern communications and electronic devices.

When early warning activities are conducted continuously as a "campaign" rather than episodically and often briefly before a crisis emerges in support of the indications and warning (I&W) mission, the insights gained into adversary capabilities, vulnerabilities, and intentions may offer a multitude of opportunities for the President to intervene left-of-launch long before a crisis matures into one where the risk of nuclear conflict is high.

To enable the creation of an integrated deterrent, several measures need to be undertaken:

- Enhancing the fusion of OSI and other intelligence information (i.e., early warning) to provide insights into opportunities for the President to take decisive and timely action to reinforce deterrence.
- The non-nuclear capabilities that can strengthen nuclear deterrence need to be integrated with the nuclear deterrent through a modernized command and control system, which facilitates the blending of an appropriate mix of capabilities as specific scenarios unfold.[6]

[6] The Task Force takes note of Russia's integration of cyber operations as part of its effort to disrupt and deter the U.S. nuclear deterrent – including cyber-attacks on U.S. weapon systems.

- The nuclear enterprise needs to become responsive and adaptive to the need to sustain the deterrent and the extended deterrent through life extension of existing weapon systems, modernization of existing nuclear weapon systems to enable them to meet the needs of the deterrent, and the ability to have the capacity to design, develop, produce, and support new nuclear weapon designs if needed in the future.[7]

Recommendations

ADAPTIVE NUCLEAR ENTERPRISE

N-1. The **Air Force** and the **Navy**, with the **Department of Energy (DOE)** and the **National Nuclear Security Administration (NNSA)**, should adapt current capabilities and programs as needed for enhanced deterrent effect.

N-2. The **Nuclear Weapons Council (NWC)** should review the joint DOE/NNSA-DoD implementation of the stockpile responsiveness program (Section 3112, FY16 NDAA).

N-3. The **Under Secretary of Defense for Acquisition and Sustainment (USD(A&S))** should direct inclusion of rapid prototyping and acquisition responsiveness in delivery system modernization, and include DOE/NNSA participation to ensure warhead-delivery system compatibility.

INTEGRATED DETERRENCE

N-4. The **Under Secretary of Defense for Policy (USD(P))** should develop integrated deterrence guidance for both combatant command (CCMD) planning and Military Department programming to ensure, or develop, a broader range of options.

N-5. The **Chairman of the Joint Chiefs of Staff** should develop a capstone requirement for the integrated mission of deterring, preventing, and responding to the threat or use of nuclear weapons.

N-6. The **Joint Staff** (across the Joint Staff) should embed integrated deterrence planning scenarios into operational planning.

N-7. The **CCMDs** must determine mission requirements for execution of Operation Plans in adversary-generated nuclear environments.

N-8. The **USD(A&S)** should restructure nuclear weapons and systems acquisition processes to facilitate and ensure ability to adapt to evolving threats.

[7] Findings and recommendations support development of a modernized nuclear enterprise that responds to Congressional Direction in the FY16 NDAA [Section 3112(2)].

EARLY WARNING ENABLES INTEGRATED DETERRENCE

N-9. The **USD(P)** should restore the analytical capability to conduct dynamic, long-view assessments to inform policy, CCMD plans, and Military Department programs.

- Establish new U.S. Government baseline – a comprehensive, cross-cutting understanding of nuclear thinking and capabilities among adversaries and potential proliferators.
- Leverage key DoD, DOE/NNSA, IC, and other supporting organizations/institutions' lines of efforts (e.g., national labs, University Affiliated Research Centers, Federally Funded Research and Development Centers, industry).

N-10. The **CCMDs, both regional and functional**, should leverage enhanced early warning to identify opportunities both early and later in the life-cycle to continue to develop and enhance country-specific, integrated deterrence campaign plans.

These should include:

- diplomatic and military activities
- "pathway defeat/network defeat" opportunities
- kinetic and non-kinetic counterforce opportunities (left-of-launch)
- defensive measures
- options to control escalation at low levels
- interagency – building on geographic CCMD and U.S. Special Operations Command (SOCOM) missions and plans

Appendix A: Task Force Terms of Reference

ACQUISITION, TECHNOLOGY AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

NOV 1 2 2014

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Deterring, Preventing, and Responding to the Threat or Use of Weapons of Mass Destruction

The underlying technologies of weapons of mass destruction [nuclear, chemical, and biological, and depending on scope, radiological, weapons] are widely known and understood. Nuclear weapons technology is more than seven decades old, and weapons capabilities have been developed by some of the most impoverished and underdeveloped nations on earth. Chemical weapons have been available for more than a century while primitive biological weapons have been used for millennia. Radiological material is readily accessible in the civil sector and its malicious distribution and may have highly disruptive effects even if it is not nearly as destructive as nuclear weapons.

The purpose of this study is to identify ways in which deterrence can evolve given a changing security environment, and should deterrence alone prove inadequate, then identify additional ways to prevent and respond, both for the United States and for its allies. The study will investigate how the threat or use of weapons of mass destruction (nuclear, chemical, biological, and radiological weapons) can be best addressed through deterrence, prevention, defense and/or response. The study will address questions as: What capabilities are available for early detection of research, development and acquisition? What technology advances are necessary to deter or prevent following early detection? How far can such advances and others that are yet to be fielded go in deterring WMD use? Will declared policies and capabilities remain sufficiently credible?

I will sponsor the study. Dr. Miriam John and Dr. William Schneider will serve as Co-chairs of the study. Christine Parthemore, (OASD/NCB) will serve as Executive Secretary. CAPT James CoBell, USN, will serve as the DSB Secretariat Representative.

The study will operate in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act" and DoD Directive 5105.04, the 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.

Frank Kendall

Appendix B: Acronyms and Abbreviated Terms

A2AD	anti-access area denial
ASD(NCB)	Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense
BDA	battle damage assessment
BW	biological weapons
CB	chemical and biological weapons
CBDP	Chemical and Biological Defense Program
CCMD	combatant command
CDC	Center for Disease Control and Prevention
CONOPS	concept of operations
CT	counterterrorism
CW	chemical weapons
CWC	Chemical Weapons Convention
CWMD	countering weapons of mass destruction
DARPA	Defense Advanced Research Projects Agency
DASD(CBD)	Deputy Assistant Secretary of Defense for Chemical and Biological Defense
DHS	Department of Homeland Security
DHA	Defense Health Agency
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DOE	Department of Energy
DSB	Defense Science Board
DTRA	Defense Threat Reduction Agency
EA	executive agent
EID	emerging infectious diseases
FDA	Food and Drug Administration
FFRDC	federally funded research and development center
HAZMAT	hazardous materials
IARPA	Intelligence Advanced Research Projects Activity
IC	intelligence community
IND	Investigational New Drugs

INT	intelligence
IPT	integrated planning team
JIATF	Joint Interagency Task Force
JPEO	Joint Program Executive Office
JSTO	Joint Science and Technology Office
NCPC	National Counterproliferation Center
NGO	non-governmental organization
NIPF	National Intelligence Production Framework
NNSA	National Nuclear Security Administration
NSA	National Security Council
NWC	Nuclear Weapons Council
ODNI	Office of the Director of National Intelligence
OHA	Office of Health Affairs
OSD(P)	Office of the Secretary of Defense for Policy
OSI	open source information
RD&A	research, development, and acquisition
SECDEF	Secretary of Defense (SECDEF)
SME	subject matter expert
SOCOM	Special Operations Command
TTP	tactics, techniques, and procedures
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
WHO	World Health Organization
WMD	weapons of mass destruction

DEFENSE SCIENCE BOARD

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
WASHINGTON, D.C. 20301-3140