



2020 DSB SUMMER STUDY ON
**NEW DIMENSIONS
OF CONFLICT**
EXECUTIVE SUMMARY


**CLEARED
For Open Publication**

May 16, 2023

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

23-S-2072

April 2023



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 Defense
Department (DoD).



**DEFENSE SCIENCE
BOARD**

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

(U) MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING

(U) SUBJECT: Final Report of the 2020 Defense Science Board Summer Study on New Dimensions of Conflict

(U) We are pleased to forward the final report of the 2020 Defense Science Board (DSB) Summer Study on New Dimensions of Conflict. This Study explored the means by which nations impose their political will, particularly outside the traditional threat or use of military force. This evolution of statecraft has created opportunities for new dimensions of conflict which present the United States with new opportunities to maintain hegemony and challenges to defend against vulnerabilities. The Study examined new dimensions such as the global information infrastructure, technology/intellectual property, international law and standards, influence/coercion, population (demographics, ethics, national identity), global engagement, and supply chain. Additionally, the Study also considered opportunities and challenges in existing warfare dimensions (e.g., sea and seabed).

(U) The report provides key recommendations to avoid future surprises and explore how such dimensions of conflict might be exploited by near-peer competitors, Russia and China, and adversaries to impose their will on other nations. The DSB considered a whole-of-government approach to address each dimension and hedge against the ability of our adversaries to exert influence counter to U.S. interests. I fully endorse all the recommendations contained in this report and urge their careful consideration and adoption.

A handwritten signature in black ink, appearing to read "Eric Evans".

Dr. Eric Evans
Chair

Executive Summary

The Defense Science Board's (DSB) 2020 Summer Study of New Dimensions of Conflict completed its work in January 2021. The impact of the Coronavirus Disease-2019 (COVID-19) and the change of administration resulted in a pause of Defense Department (DoD) advisory board activities and delayed DoD approval and publication of the 2020 report until the DSB was reestablished on July 2, 2021. Much has happened in the intervening time related to this subject and this Executive Summary highlights the continued relevance of the report's findings and recommendations.

Recent events include:

- Russia's invasion of Ukraine underlies the shift in Russian post-Cold War strategic aims to build a unified Eurasian State based on Russian ethnicity.
- Institutionalization of the China-Russia strategic alliance with the signing of the Joint Declaration and its accompanying "no limits" pronouncement.
- China and Saudi Arabia signed a "Comprehensive Strategic Agreement" that integrates Chinese and Saudi economic and security interest. Saudi Arabia also agreed to align its long-term development plan, *Saudi Arabia 2030* with China's Belt and Road Initiative (BRI).
- Renewal and enlargement of the North Atlantic Treaty Organization (NATO) alliance structure with Finland and Sweden motivated by the Russian invasion of Ukraine. The United States Indo-Pacific Command (USINDOPACOM) security relationships have been strengthened by the conclusion of the Australia-United Kingdom-United States (AUKUS) Agreement, the Quadrilateral Dialogue (Australia-India-Japan-United States (U.S.)), and increased NATO naval presence in the region.
- Increasing, perhaps unprecedented, employment of sanctions and related financial, trade, and technology measures targeting Russia (and Belarus) have proven to be less effective as a deterrent than as a means of diminishing adversary defense-industrial resilience.
- Increasing importance of the "information war" on many fronts including Ukraine's adept use of such instruments and Russia and China's continued internal censorship.
- The globalization of China's surveillance and coercion capabilities through Identity Exploitation and Control (IEC) to target individuals.
- China's initiation of a large-scale expansion of its strategic nuclear forces described by the Commander of the U.S. Strategic Command as a "nuclear breakout" as a dimension of its capacity for coercive diplomacy.
- Russia's manipulation of the coercive threat or use of weapons of mass destruction (WMD) in the Ukraine crisis may stimulate other nuclear states to deter U.S. intervention in a conventional conflict if a non-treaty ally is involved.

Russia and China have become adept at operating sustained campaigns in the gray zone¹, using dimensions of conflict different from traditional kinetic combat operations and gaining benefits without suffering significant consequences. Putin’s invasion of Ukraine was emboldened by his successes using a combination of gray zone² tactics and combat operations: in Chechnya, Georgia, Belarus, Crimea, Syria, and by assassinations on foreign soil, interference in U.S. and other nations’ elections and use of “little green men.” China is operating in the gray zone to resolve territorial claims (India and Taiwan) and commingle its Belt and Road Initiative infrastructure projects with its security aspirations. Their instruments for manipulating national power, economic and financial resources, arms transfers, etc. are often complementary, mutually supporting in gray zone campaigns and not always readily attributed. A consequence of the institutionalization of Sino-Russian collaboration is each nation’s “inherited” alliance relationships. For example, their shared association with Iran will present greater challenges to U.S. interests in the Gulf region.

China and Russia seek regional and global hegemony, though neither now has the capability to impose political will globally by military means (however, China may be striving for such capability). Both countries have developed new means of projecting their influence globally; in short, new dimensions of conflict. These new dimensions of conflict give them the capability for expanding global influence without the challenge and substantial expense of global military reach; give them capabilities that asymmetrically sidestep direct military conflict with the U.S. which they would likely lose; and give them capabilities that are difficult for the U.S. to counter and mitigate consistent with American values and norms.

These dimensions of conflict can be employed in complex ways over time in the form of “campaigns” that can long precede kinetic operations and may be able to achieve objectives without resorting to kinetic means. Thus, gray zone competition will remain a major element of major power competition, as a substitute, an enabler and a complement to kinetic operations.

The 2022 National Defense Strategy (NDS) stresses the importance of gray zone competition and the opportunities of DoD of integrating its actions “with the actions of allies, partners, and other U.S. departments and agencies.” The 2022 NDS parallels a key finding of this DSB report, the significance of planning and executing campaigns. The NDS acknowledges the limits of traditional military tools in “countering competitors’ coercive behavior in gray zone operations.” It states that, “in many cases, intelligence sharing, economic measures, diplomatic actions, and activities in the information domain conducted by other U.S. departments and agencies may prove more effective. Nevertheless, there can be an important role for campaigning to disrupt competitors’ attempts to advance their objectives through gray zone tactics, especially when integrated for maximum impact with the actions of allies, partners, and other U.S. departments and agencies.”³

1. In the gray zone adversary nations compete below open combat using an array of tactics including economic coercion, cyber espionage, disinformation and unattributed military forces.

2. Additional discussion of gray zone competition can be found in the DSB’s *Capabilities for Constrained Military Operations* and the Center for Strategic and International Studies’ *Gray Zone Project*.

3. Defense Department, *2022 National Defense Strategy*, (Washington, DC: Defense Department, 2022), 12, <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>.

This report identifies five emergent possibilities worthy of proactive attention, describes these new dimensions of conflict, and recommends what to do about them. The five, new in the sense that technology and the geopolitical environment have amplified their impact, are:

- Identity Exploitation and Control.
- China's attempt to control the evolution of the Global Information Infrastructure (GII).
- Challenge to freedom of the seas and seabed.
- Threats to global supply chains.
- China and Russia's whole-of-society global engagements that seek to undermine U.S. relations with allies, partners, and friends.

The five new dimensions of conflict are already being supplemented by other aspects of conflict; and the U.S. Government (USG) needs to institutionalize processes to prepare for these potential challenges. Moreover, these dimensions of conflict are not single events but are implemented as campaigns that extend for months or years so long as they achieve the user's aims. Consequently, the report also recommends steps that DoD and the USG should take action to better cope with and create surprise. Of note is slow surprise, when an adversaries' salami slice strategy unexpectedly emerges as a major threat. The need for a more proactive posture is a major theme of the report.

Identity Exploitation and Control (IEC) May Be the Most Difficult of the Five New Dimensions of Conflict to Counter

The ability to collect, process, and exploit comprehensive data on individuals and groups has accelerated in recent years at unprecedented levels of speed, scale, and precision. Thus, these age old techniques have transformed into a major strategic tool for gaining advantage across all phases of competition and conflict.

Medical, health, financial, behaviors, affiliations, genetic profiles, social interactions, location history are some of the data available. Strategically important individuals and groups across the globe—in government, military, industry, and media—can be targeted. Identity exposes vulnerabilities that adversaries can exploit to damage U.S. interests by coercing, bribing, threatening, distracting or tricking them, stealing their authority or faking their apparent actions to destroy reputations.

China is using these new means of identity exploitation and control to pursue dissidents and non-Han Chinese minorities including Mongols, Tibetans, and Uyghurs. China also is leveraging its global harvest of data on individuals to expand its reach to target and manipulate individuals on a global scale including more than 10,000 living outside of China. Russia is adopting key elements of China's domestic surveillance system including Huawei telecom equipment. While this does not change the scale of China's IEC, it leverages Russia's cyber skill-sets and can propagate a worldwide China-Russia IEC threat.

China's Seeks to Control the Evolution of the Global Information Infrastructure (GII)

The GII, providing applications and information connecting people, companies and nations worldwide, is an enabler of IEC. It has also become a domain of conflict itself.

China's success would foster the global spread of authoritarian power and undermine U.S. relations with allies, partners and countries of strategic interest. The result could be as consequential as other historical global hegemonies such as Britain's rule of the seas in the 19th century. Envision a world where an authoritarian government surveils, controls, or intervenes in all digital transactions: commerce, education, social, trade, health care, government, i.e., the current situation in Xinjiang Province on a global scale.

Their strategy is comprehensive. Its means include control of technical standards, patents, components and systems and intellectual property theft.

One example is the Digital Silk Road (DSR) introduced in 2015 as a component of China's Belt and Road Initiative. It is a set of telecommunications and data-related projects supporting BRI development. These investments often include a significant amount of sovereign debt being imposed on the included nations. China intentionally extends excessive credit to a debtor country often linking loans to sovereign resources, such as ports and mines, as a means of collateral. These resources will come under Chinese control when that country becomes unable to honor its debt obligations. Another is Huawei's attempt to build Chinese-controlled undersea fiber cable to facilitate its exploitation of telecommunications networks.

Fifth generation (5G) networks provide dramatic improvements in speed, latency, and connectivity and offer the potential for transformative impacts on telemedicine, education, autonomy, augmented and virtual reality, and many other applications. It is essential for the U.S. to lead in this domain for economic, societal, and security reasons.

The institutionalization of Sino-Russian collaboration as a result of the 2022 "no limits" bilateral agreement, their collaboration has in the GII is now coordinated. China has adopted the rhetoric and activism of Russia's anti-NATO crusade, while Russia is supporting China's position on Taiwan through both diplomatic and information infrastructure channels. China and Russia's shared diplomatic, economic, and military collaboration extends to other nations with an anti-U.S. agenda. Both China and Russia have nearly identical long-term economic and military cooperation agreements with Iran, and both nations collaborate with the Democratic People's Republic of Korea (DPRK) to evade United Nations (UN) sanctions.

Russian submarines and its "Special Purpose Ship," the Yantar, have an affinity for loitering around undersea cables. In January 2022, Admiral Sir Tony Radakin, head of the United Kingdom's Armed Forces, warned that Russia could "put at risk and potentially exploit the world's real information system, which is undersea cables that go all around the world."⁴

4. PA Media, "UK military chief warns of Russian threat to vital undersea cables," *The Guardian*, January 8, 2022, <https://www.theguardian.com/uk-news/2022/jan/08/uk-military-chief-warns-of-russian-threat-to-vital-undersea-cables>.

A comprehensive set of actions are needed to deal with three fundamental risks to the GII. These risks involve:

- Loss of control: inability to manage network operations, routing, availability, and performance; conversely, ability for unauthorized parties to exert control at times of their choosing.
- Loss of integrity: interference with content of data sent over network connections.
- Loss of mandate: inability to have major influence on the evolution of technology components, standards, and priorities.

China and Russia Continue to Threaten Freedom of the Seas and Seabed

New aspects include the growing importance of the Arctic Region, emerging undersea technology and China's use of its BRI. Among the more recent manifestations are:

- Chinese control of choke points (e.g., Bab-el-Mandeb and Djibouti at the Red Sea and China's lease of Iran's Kish Island in the Straits of Hormuz) that pose a risk to U.S. and allied naval access. China now controls at least 100 ports in 63 countries.
- China reportedly is seeking a naval base in Equatorial Guinea that would be their first military base on Africa's Atlantic coast.
- China's activism in the Central and South Pacific islands highlighted by the China-Solomon Islands Security Pact that permits China to establish a military presence there as well as longterm leases of islands within the archipelago. The included approximately 900 islands sit astride major shipping lanes.
- China is expanding the Ream Naval base in Cambodia after extensive involvement in modernizing Cambodia's infrastructure. The naval base will enable China to complement its naval forces in Northern region of the South China Sea based Hainan, China, with naval combatant vessels at Ream close to the Southern part of the South China Sea.
- China's presence in Central America builds on its port infrastructure at the Northern (Cristobal Port) and Southern (Balboa Port) end of the Panama Canal.

While Russia's goal to convert the Arctic into its own territorial river seaway was setback from the effect of sanctions on shipping orders, the effect will be transitory. Russia's Arctic ambitions remain. China also seeks to become an Arctic player and published 'China's Arctic Policy' in 2018.⁵ The most recent U.S. national Arctic strategy was released in 2022 and with the 4 pillars of *Security, Climate Change and Environmental Protection, Sustainable and Economic Development, and International Cooperation and Governance*.⁶ This new national strategy commits to whole-of-government approach, cultivation of public/private partnerships, and collaboration with allied

5. People's Republic of China, China's Arctic Policy, January 2018, https://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm.

6. The White House, National Strategy for the Arctic Region, October 2022, <https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Strategy-for-the-Arctic-Region.pdf>.

nations. The prospect that Finland and Sweden will join NATO aids strengthening of the U.S. and allied position in the Arctic region.

A key recommendation of the report is to restore DoD's maritime systems' operational readiness to high levels, a necessary step to maintain freedom of the seas, deter and defeat a near-peer adversary in the maritime domain. This recommendation concerning operational readiness is what needs to be done in addition to executing the shipbuilding and modernization plan. Failure to maintain operational readiness is a *de facto* decrease in the size of the fleet.

Globalization of the Supply Chain has Enabled the Weaponization of Interdependence

Supply chains can be disturbed by natural disasters, unplanned or poorly planned mismatch between supply and demand, or by malicious action by nations' attempting to impose their will on others.

The latter is the focus here and describes how a supply chain attack can occur in any industry or sector. Such attacks can deny and/or degrade the integrity of critical materials/capabilities for military use, products for population safety and security and materials/capabilities affecting economic prosperity. Attacks can also target confidence in the supply chain integrity (beyond counterfeit parts) where malicious inserts or replacements are injected for later exploitation. The global reach of the emerging capability to exploit and control individuals (IEC) offers additional paths to threaten supply chains.

Traumatic disruptions of global supply chains have occurred in the past few years. First from the COVID pandemic. And now followed by Russia's invasion of Ukraine when Russia weaponized the sale of oil and natural gas to Europe. According to a White House June 17, 2021, report, more than 60% of the U.S. manufacturing sector has been disrupted by supply chain difficulties produced by the global pandemic and international trade disruptions.⁷ A 2021 survey by The Economist Intelligence Unit found that supply chain disruptions may have produced a loss of \$4 trillion in industry revenue.⁸ These disruptions have had and will continue to have significant consequences for the DoD's industrial base.

A major of concern is that in most cases the U.S. lacks visibility in the lower tiers of supply chains critical to its economy and security nor to identify the beneficial owners of its suppliers. This concern is reinforced by the November 2021 McKinsey & Co. article *How COVID-19 is Reshaping Supply Chains*. It found that almost half of a diverse group of companies spanning multiple industries (including aerospace and defense) had visibility into the first tier of their supply base but only two percent had visibility beyond the second tier.⁹ This was a year after almost all the companies were planning to

7. The White House, *Why the Pandemic Has Disrupted Supply Chains*, Susan Helper and Evan Soltas, June 17, 2021, https://www.whitehouse.gov/cea/written-materials/2021/06/17/why-the-pandemic-has-disrupted-supply-chains/#_ftn2.

8. Economist Economic Intelligence Unit, *Up to \$4 Trillion in Revenue May Have Evaporated in Supply Chain Disruptions*, NEW GEP Commissioned Survey of U.S. & European BIZ Chiefs Reports, *News Release*, March, 24, 2021, <https://www.gep.com/prod/s3fs-public/files/newsroom/docs/up-to-4-trillion-dollar-in-revenue-may-have-evaporated-insupply-chain-disruptions-new-gep.pdf>.

9. Knut Alicke, Ed Barriball, "How COVID-19 is Reshaping Supply Chains," *McKinsey & Company*, November 23, 2021, <https://www.mckinsey.com/capabilities/operations/our-insights/how-covid-19-is-reshaping-supply-chains>.

make their supply chains more flexible, agile, and resilient. Critical components such as microelectronics depend on these lower tiers.

The administration and the Congress are beginning to address this threat. In February 2022, DoD published “Securing Defense-Critical Supply Chains: An action plan developed in response to President Biden’s Executive Order 14017”.¹⁰ This is a first step towards our report’s finding that DoD needs an overarching strategy incorporating the supply chain as a new dimension of conflict embracing its defensive, offensive, and deterrence aspects. The report’s recommendations concerning “ally shoring” to extend the scope of the U.S. defense industrial base to include the scientific and industrial capabilities of close allied and friendly nations can be particularly valuable supporting the aims of the U.S. “integrated deterrence” policy.

Competition for Global Relationships has Continued for Millennia — However, the U.S. Confronts New Challenges

China and Russia are united in the goal of thwarting U.S. interests. China has the financial clout to operate globally offering enticing economic relationships and then following with political and military. Russia leverages its oil and gas resources to influence the behavior of other nations as well as offers military aid.

China opportunistically exploits its BRI presence to expand its regional security footprint, to diminish U.S. influence, undermine Taiwan’s economic and diplomatic presence, and to entrench its long-term presence through its permanent local operation of Chinese infrastructure projects. Chinese involvement in BRI infrastructure in the Philippines is commingled with threats to Philippine sovereignty in the South China Sea. Chinese and Russian activity in resource-rich African nations can reduce U.S. and allied access to resources.

Closer to home are China’s activities in Latin America and the Caribbean (LAC). China is already the major trading partner of several nations including Argentina and Brazil. Twenty-one LAC nations have signed up for the BRI. The engagements go beyond economic. China has sold military equipment to several LAC nations and China has established a high-level defense forum with the Community of Latin American and Caribbean States (CELAC). In El Salvador, China’s BRI presence involves a mix of trade, telecommunications, infrastructure, and related initiatives.

Strengthening global relationships is a pervasive theme of the report. It is also central to the recommendations on threats to the GII, freedom of the seas and supply chains. Recent events presage the greatest opportunity since 9/11 to strengthen these relationships. These events, some considered quite unlikely not too long ago, include renewal of the NATO alliance structure, the unprecedented employment of sanctions targeting Russia, increased interest in Finland and Sweden in NATO

10. Defense Department, Securing Defense-Critical Supply Chains: An Action Plan Developed in Response to President Biden’s Executive Order 14017, February 2022, <https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF>.

membership, the Australia-UK-U.S. Agreement, the Quadrilateral Dialogue (Australia-India-Japan-U.S.), increased NATO naval presence in the Indo-Pacific.

Lessons can be learned about how the U.S. can enhance the defense capacity and capability of allies, partners and nations of strategic interest. Combat operations that began in Ukraine in 2014 were preceded by two decades of Ukraine's participation in the National Guard's State Partnership Program. While each nation's partnership has unique features, the lessons from Ukraine (and the 2020 Azerbaijan/ Armenia War) can inform U.S. efforts in other nations. This could entail creating contingency plans for potential expansion of cooperation and support.

The value of engagements with allies and partners flows both ways. It took decades during the Cold War to grow the depth and breadth of Kremlinologists throughout the USG, academia, and industry, building on the expertise of George Kennan. That resource has atrophied since the end of the Cold War. U.S. allies and partners living closer to Russia can greatly deepen understanding of their values, intent and capabilities. Furthermore, allies and partners can significantly enhance early warning of specific Chinese and Russian gray zone activities while amplifying the effectiveness of U.S. measures to advance national interests below the level of kinetic conflict.

Effective U.S. and allied responses are needed to address Chinese and Russian practices of commingling diplomatic, economic, and financial instruments with commercial entities, private military contractors, and overt military presence in contested regions. These current practices differ from Cold War experience and practice. China and Russia may also interact with selected allies such as the DPRK and Iran to facilitate their opportunistic exploitation of U.S. and allied disputes with China and Russia. Russia's global engagements motivated some nations to abstain from taking action against Russia after it invaded Ukraine.

Surprise is Inevitable, Strategic Failure is Not

Surprises keep coming. More are on the way:

- The performance of Russian military (overvalued materiel and technology, undervalued culture and training).
- European nations' immediate support of Ukraine (supplying weapons, increasing defense budgets, accepting economic pain), and the commitment of the nine East European NATO Member States to a NATO shift to forward deployment in the region. Such a move would shift center of NATO military presence from the Fulda Gap in Germany to the Suwalki Gap in Poland.
- NATO's recognition of China's threat to alliance security, and support for the forward presence of NATO Member States in the Indo-Pacific region.
- U.S. allies support of tough sanctions.
- Finland and Sweden's request for NATO membership (Article V worth more than a partnership).
- Chinese and Russian success using their "allies"—Iran and North Korea—to support their aims elsewhere in the world. For example, Iran supplying drones and missiles to Russia and North Korea sending artillery ammunition to replace Russia's stocks depleted in its attack on Ukraine.

- Russian effort to “change the game” by its manipulation of nuclear threats in Ukraine that suggests possible pre-emptive use of nuclear weapons in the current conflict and signifies a change from its June 2020 Basic Principles of the State Policy of the Russian Federation on Nuclear Deterrence.

DoD must view surprises as expected, not as anomalies. Strategic surprise occurs when a nation is caught unprepared for events or circumstances resulting in great harm to its national interests. Such surprises arrive in various forms: Albert Wohlstetter’s “bolt from the gray” to situations where the cumulative effects accrue to a “surprise.” This second type (slow surprise) is a likely outcome of campaigns in employing new dimensions of conflict receiving leadership attention only when they have become big problems. There are many possible reasons for being surprised but almost never because there was no warning. Historical cases show that political and psychological impediments are the primary blinders.

The report provides recommendations about coping with and creating surprise. These involve more frequent challenge of assumptions underlying strategies, plans and programs; more adaptive planning and programming processes; more use of hedges; more red teaming and gaming. It will also involve changes to professional education, both uniformed and civilian.

Preparing for and adapting to surprise is necessary but hardly sufficient. An initiative-taking posture is essential. A capability to surprise adversaries should be an essential part in the nation’s national security toolkit, available to spring when opportunities arise. There will always be risks, to be managed, not avoided. The administration’s public use of intelligence data about Russia’s intentions and capabilities vis à vis Ukraine to help the U.S. shape the narrative serves as a compelling example of such risk assessment.

The shifts called for in this study will take the Secretary of Defense’s (SecDef’s) personal commitment and persistence to ask the hard questions: “Are we doing the right things?” “What if we’re wrong?” And to protect those who pose and answer these questions.

Integration of All Elements of National Power is Necessary to Support Long-Term Campaigns of Deterrence and Containment

U.S. adversaries employ such campaigns, e.g., Russia’s territorial expansion, China’s BRI and its goal to control the evolution of the GII.

The Cold War’s early years offer examples of successful whole-of-government campaigns: nation-building in Germany and Japan, the Marshall Plan, creation of NATO, Berlin airlift, Radio Free Europe/Radio Liberty, overt and covert actions to diminish communist influence in Italy and France, Truman Doctrine and defense build-up. The eighties provide another example. In these cases, the military played a central role and not merely the option of last resort. Military escalation options coupled to sound declaratory postures were central.

DoD needs to rediscover its lost art of integrating operational concepts, technology, experimentation and demonstrations to generate new capabilities to surprise adversaries, attack their strategies and put them on the defensive. Examples from the late seventies and eighties include the Air Land Battle and the U.S. Naval exercises starting with Ocean Venture 81.

The preeminence of the cognitive over the physical is fundamental to deterrence. Deterrence is about assumptions, perceptions, and messaging.

- Assumptions that U.S. leaders make about what leaders of other nations hold dear that the U.S. can hold at risk to impose costs greater than expected benefits from their aggression.
- Perceptions held by leaders of countries of U.S. capabilities and the intent and willingness of U.S. leaders to make use of the capabilities in various circumstances.
- What messages (communication strategy) will convey credible capabilities, intent and willingness to carry out threats and thus influence perceptions of foreign leaders.

What initiatives can DoD take in this arena, often as the supporting organization? A whole-of-society effort to counter this threat. For example, the DoD can take a lead in facilitating well designed, well executed, and well attended games and exercises needed to inform decisions about whole-of-government campaigns.

The U.S. leadership has long recognized the need for engaging the whole-of-government capabilities to respond the multi-dimensional challenges posed to U.S. and allied interests. The U.S. has been unable to effectively engage the whole-of-government in these challengers for institutional rather than policy reasons. A national security lever parallel to the *International Emergency Economic Powers Act* would provide the President with the flexibility to manage USG authorities, resources, and personnel in an acute crisis to achieve an integrated whole-of-government response.

Conclusion

Both China and Russia have demonstrated that they have long-term aspirations that cannot be engaged through crisis-specific conflicts. China has a plan for enabling it to become the world's dominant economic and military power by mid-century. Russia may still be seeking to create a "Russian-world" built on the territorial expanse of Tsarist Russia and the Soviet Union that is a multi-decadal undertaking beginning with its partial annexation of Georgia (2007) and Ukraine/Crimea (2014).

Appendix A: Terms of Reference



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

CLEARED
For Open Publication

Dec 31, 2019

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DEC 19 2019

MEMORANDUM FOR THE CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board 2020 Summer Study on New Dimensions of Conflict

For millennia, the most common means of imposing political will has been the threat or application of military force. In more recent times, states have employed other means to impose their political will. For example, cyber espionage and cyber attacks have become commonplace. In addition, states have used proxies (terrorist organizations, organized crime), resources (oil, natural gas), “foreign aid,” infrastructure, and private industries to further their interests, in many instances, counter to those of the United States and its allies.

Many in the United States’ political leadership were surprised by the coordination and sophistication of these new “attacks.” As a consequence, the United States and its allies were unable to develop effective strategies and doctrine for “combat” in these new dimensions of conflict, and they have since been working to counter these new tactics.

Considering this recent evolution of statecraft, it is logical to assume that as technology advances, as the world climatically and geographically changes, and as states become richer or poorer and younger or older, that new dimensions of conflict will arise that present both new opportunities and new vulnerabilities. These new dimensions might include technology/intellectual property, biology (gene editing, manipulation of higher organisms), international law (“lawfare,” international standards), influence/coercion (artificial intelligence, deepfakes), population (demographics, ethics, national identity), and academic/higher-education (Thousand Talents Program). It is also anticipated that a rapidly changing world will give rise to new opportunities and vulnerabilities in the existing warfare dimensions of land, sea, air, space, and information.

To avoid future surprises, I am tasking the Defense Science Board (DSB) to consider future dimensions of conflict that might be exploited by our near-peer competitors, Russia and China, and adversaries to impose their will on other states. The DSB should consider any new dimension wherein our strategic competitors or adversaries have both the intent and potential capability to operate and exert influence counter to U.S. interests. For each potential new dimension identified by the DSB, the DSB should recommend early-warning indicators that should be monitored to provide the longest possible lead time to develop countermeasures, new strategies, and doctrine.

Critical to this effort will be an assessment of how the Department’s R&E priorities align against these future dimensions. Therefore, I am tasking the DSB to work closely with the Modernization Directorate, and all supporting Assistant Directors, in the creation of this study. I expect a range of recommendations on how best to posture the Department to foster the brand of

20-S-0522

foresight and innovation require to go beyond merely recognizing new dimensions of conflict, and instead, be the drivers of new dimensions of conflict.

In addition, the DSB should recommend inoculating actions the United States might take, employing all the powers of state, if necessary, and provide lead times for those actions.

This summer study will be sponsored by me as the Under Secretary of Defense for Research and Engineering (USD(R&E)). The study members are granted access to those Department of Defense (DoD) officials and data necessary for the appropriate conduct of their study. As such, the Office of the Secretary of Defense and Component Heads are requested to cooperate and promptly facilitate requests by DSB staff regarding access to relevant personnel and information deemed necessary, as directed by paragraphs 5.1.8 and 5.3.4 of DoD Instruction 5105.04, "Department of Defense Federal Advisory Committee Management Program," and in conformance with applicable security classifications. 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 DSB will operate in accordance with the provisions of the Federal Advisory Committee Act (5 United States Code (U.S.C.), Appendix); Deputy Secretary of Defense memorandum, "Advisory Committee Management," dated November 26, 2018; and DoD Instruction 5105.04, "DoD Federal Advisory Committee Management Program." Individual DSB members do not have the authority to make decisions or recommendation on behalf of the DSB nor report directly to any Federal representative. It is not anticipated that this study will need to go into any "particular matters" within the meaning of title 18 U.S.C., section 208, nor will it cause any member to be placed in the position of action as a procurement official.



Michael D. Griffin

Appendix B: Study Membership

DSB Chairman	
Dr. Eric Evans	MIT Lincoln Laboratory
Study Leads	
Dr. Theodore Gold	Private Consultant
Hon. William Schneider, Jr.	International Planning Services, Inc.
DSB Secretariat	
Mr. Kevin Doxey	DSB Executive Director
Ms. Elizabeth Kowalski	Technical Advisor
Mr. David Moreau	Technical Advisor
Mr. Danny Wilmoth	DSB Staff
DSB Members	
Dr. Amy Alving	Private Consultant
Dr. Michael Anastasio	Private Consultant
Hon. Michael Bayer	Private Consultant
Mr. Frank Cappuccio	Cappuccio & Associates, LLC
Mr. James Carlini	Leidos
Dr. Victoria Coleman	Private Consultant
Gen. Michael Carns, USAF (Ret.)	Private Consultant
Hon. David Chu	Private Consultant
Dr. Ruth David	Private Consultant
Mr. Christopher Day	Cyxtera, Inc.
Dr. William Delaney	MIT Lincoln Laboratory
ADM William Fallon, USN (Ret.)	Private Consultant
Dr. Craig Fields	Private Consultant
Mr. James Gosler	JHU Applied Physics Laboratory
Mr. Alfred Grasso	Private Consultant
Hon. Paul Hooper	Private Consultant
Ms. Jill Hruby	Private Consultant
Brig. Gen. John (Chris) Inglis, USAF (Ret.)	U.S. Naval Academy
Hon. William Jeffrey	SRI International
Dr. Miriam John	Private Consultant
Hon. Anita Jones	Private Consultant
Hon. Paul Kaminski	Technovation, Inc.
Mr. Daniel Kaufman	Google
Dr. Ronald Kerber	Private Consultant
GEN. Paul Kern, USA (Ret.)	The Cohen Group
Hon. William LaPlante	Draper Laboratory
Dr. John Manferdelli	Northeastern University
Dr. Mark Maybury	Stanley Black & Decker
Hon. Judith Miller	Private Consultant
Mr. Robert Nesbit	Private Consultant
Dr. Paul Nielsen	Carnegie Mellon, Software Engineering Institute
Dr. Michael Pazzani	University of California

DSB Members	
Mr. Michael Rich	RAND Corporation
Mr. Mark Russell	Raytheon
Dr. Ralph Semmel	JHU Applied Physics Laboratory
Mr. James Shields	Private Consultant
VADM Edward (Ed) Straw, USN (Ret.)	Osprey Venture Partners, LLC
Dr. James Tegnelia	Private Consultant
Hon. David Van Buren	Crossroads Management
Mr. Lou Von Thae	Battelle
Dr. Robert Wisnieff	IBM

Subject Matter Experts	
Mr. Jonathan Bierce	JHU Applied Physics Laboratory
Hon. Kari Bingen	Center for Strategic and International Studies
Mr. Bradford Boston	Private Consultant
Dr. David Brown	Lawrence Livermore National Laboratory
Col. Robert Butler, USAF (Ret.)	Institute for Defense Analyses
Dr. T. Charles Clancy	The MITRE Corporation
Dr. Dean Collins	Institute for Defense Analyses
Dr. Tomás Diaz de la Rubia	University of Oklahoma
Mr. Michael DiRossi	JHU Applied Physics Laboratory
Mr. Nicholas Efthimiades	Penn State University
Mr. Robert Giesler	Private Consultant
Dr. John Gronager	The MITRE Corporation
Dr. Jerry Hendrix	The Telemus Group
Mr. William Kenwell	Private Consultant
Dr. Edlyn Levine	The MITRE Corporation
Ms. Jeannette Manfra	Google
Dr. Jason Matheny	Georgetown University
Dr. Michael McGrath	Private Consultant
Dr. Jennifer Moroney	RAND Corporation
Dr. Leonard Napolitano	Lawrence Livermore National Laboratory
Ms. Sezin Palmer	JHU Applied Physics Laboratory
Lt. Gen., Dr. Robert Schmidle, USMC (Ret.)	Arizona State University
Mr. Troy Thomas	Boston Consulting Group
Dr. Richard Wagner	Private Consultant
Dr. Kevin Woods	Institute for Defense Analyses

Government Advisors	
Mr. Jim Baker	Office of Net Assessment
Mr. Justin Buelato	National Security Agency
Mr. Koreyan Calloway	Office of the Under Secretary of Defense (Policy)
Dr. Nils Carlson	Office of the Director of National Intelligence
Ms. Joyce Corell	Office of the Director of National Intelligence
Dr. David Epstein	Office of Net Assessment
Mr. Daniel Flynn	Office of the Director of National Intelligence
Dr. Rebecca Goolsby	U.S. Navy
COL Lee Grubbs, USA (Ret.)	U.S. Army
Mr. Evans Hartman	U.S. Navy

Government Advisors	
Mr. Jason Hogue	National Security Agency / U.S. Cyber Command
Dr. Richard Joseph	U.S. Air Force
Col. Sam Kinch	U.S. Cyber Command
Dr. James Lacey	U.S. Marine Corps
Ms. Monica Miller	U.S. Special Operations Command
Ms. Katherine Nikas	Senate Armed Services Committee
Mr. Charles Osborn	Defense Information Systems Agency
CAPT Jeff Ragghianti	U.S. Navy
Dr. Daniel Ragsdale	Office of the Under Secretary of Defense (Research & Engineering)
Ms. Annette Redmond	Department of State
Dr. Dakota Roberson	Defense Department
Dr. Thomas Rondeau	Defense Advanced Research Projects Agency
Mr. David Ross	U.S. Air Force
Dr. Jonathan Smith	Defense Advanced Research Projects Agency
Mr. James Stahlman	Office of the Under Secretary of Defense (Policy)
Dr. James Trebes	Office of the Under Secretary of Defense (Research & Engineering)
CAPT Matt Verich	Office of Naval Intelligence
Dr. Chad Waddington	U.S. Air Force
Mr. Phillip Walter	U.S. Air Force
CAPT Edward Westfall	U.S. Coast Guard
Mr. Neal Ziring	National Security Agency
LtCol Matthew Zulauf	Office of Net Assessment

Analytical Support	
Ms. Elizabeth Armistead	Strategic Analysis, Inc.
Ms. Carrie Bayer	Strategic Analysis, Inc.
Ms. Amy Cauffman	Strategic Analysis, Inc.
Mr. Kevin Gates	Strategic Analysis, Inc.
Ms. Ashlee Gilligan	Strategic Analysis, Inc.
Mr. Marcus Hawkins	Strategic Analysis, Inc.
Ms. Shannon Keys	Strategic Analysis, Inc.
Ms. Jamileh Mogin	Strategic Analysis, Inc.
Ms. Jamie Pilot	Strategic Analysis, Inc.
Ms. Hannah Schmidt	Strategic Analysis, Inc.
Dr. Adrian Smith	Strategic Analysis, Inc.
Ms. Melissa Smittle	Strategic Analysis, Inc.
Mr. Theodore Stump	Strategic Analysis, Inc.
Mr. Zachary VanSice	Strategic Analysis, Inc.

Appendix C: Acronyms and Abbreviations

5G	fifth generation
ASEAN	Association of Southeast Asian Nations
AUKUS	Australia-United Kingdom-United States
BRI	Belt and Road Initiative
CELAC	Community of Latin American and Caribbean States
COVID-19	Coronavirus Disease-2019
CUI	Controlled Unclassified Information
DoD	Defense Department
DPRK	Democratic People's Republic of Korea
DSB	Defense Science Board
DSR	Digital Silk Road
GII	Global Information Infrastructure
IEC	Identity Exploitation and Control
LAC	Latin America and the Caribbean
NATO	North Atlantic Treaty Organization
NDS	National Defense Strategy
SecDef	Secretary of Defense
UK	United Kingdom
UN	United Nations
U.S.	United States
USG	U.S. Government
USINDOPACOM	United States Indo-Pacific Command
WMD	weapons of mass destruction
