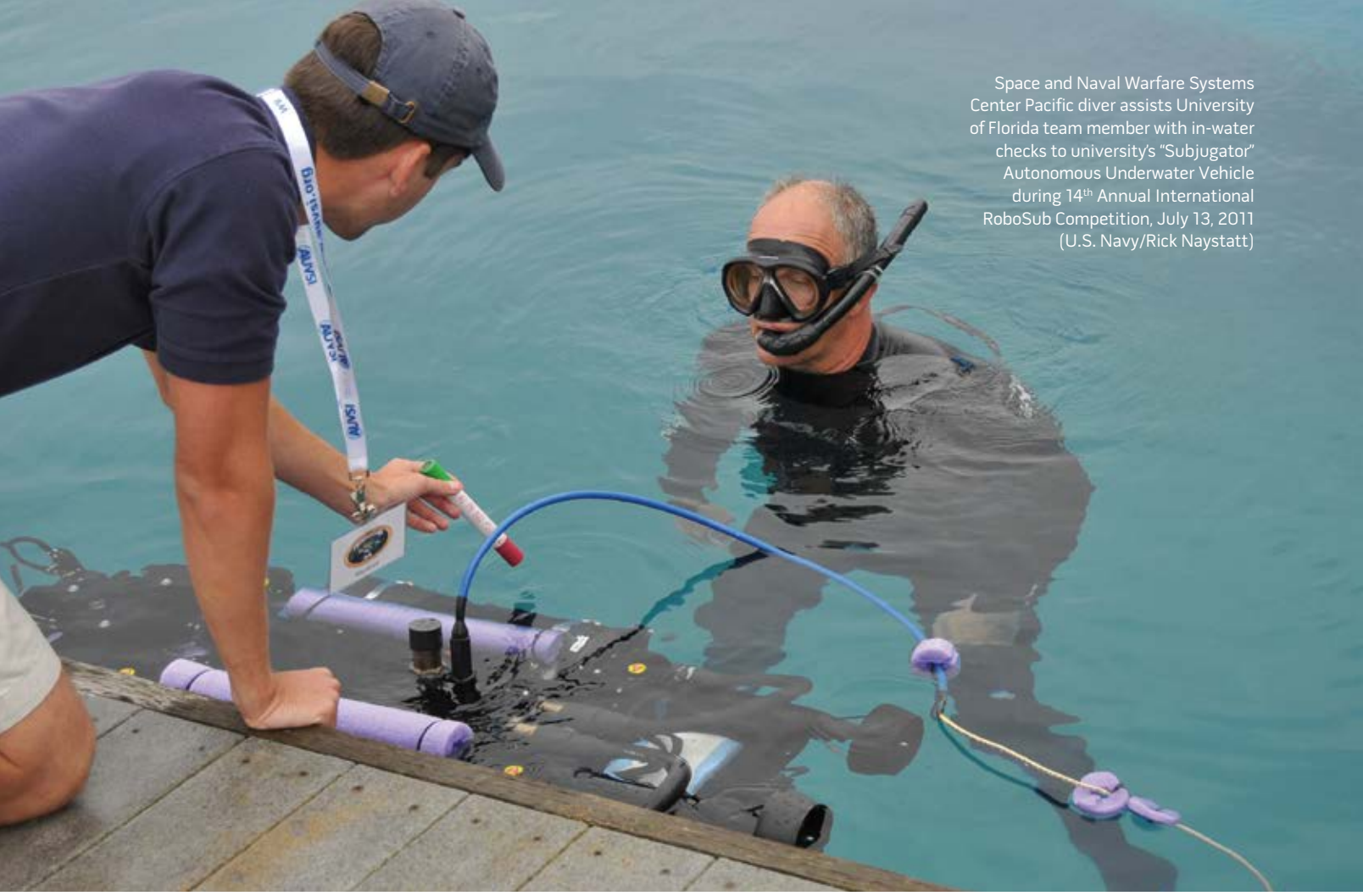

Space and Naval Warfare Systems Center Pacific diver assists University of Florida team member with in-water checks to university's "Subjugator" Autonomous Underwater Vehicle during 14th Annual International RoboSub Competition, July 13, 2011 (U.S. Navy/Rick Naystatt)

Global Power Distribution and Warfighting in the 21st Century

By John R. Benedict, Jr.

The U.S. national security community needs to focus more on the driving forces and likely associated consequences that will influence warfighting in the 21st century. A disproportionate amount of effort is spent by national security experts on narrow problem and solution spaces without an adequate appreciation of broader trends and potential shocks that could dramatically change U.S. national security perspectives. By largely ignoring these longer term factors, the U.S. military is unlikely to develop the needed national defense capabilities to deal effectively with critical threats in this emerging environment. With even greater fiscal constraints predicted for the U.S. Department of Defense (DOD) in the decades to come, it is crucial that U.S. military forces and their capabilities be properly aligned to counter a wide spectrum of threats and challenges that could undermine U.S. national security interests in the first half of this century and beyond.

John R. Benedict, Jr., is a Fellow in the National Security Studies Office and former Head of the Joint Warfare Analysis Branch within the National Security Analysis Department at The Johns Hopkins University Applied Physics Laboratory.

Drivers and Trends for U.S. Security

The first driving force that deserves more recognition is the nature and diffusion of power globally. U.S.

power is less influential and dominant than it was from World War II to the immediate post–Cold War era. In many instances "coalitions of the willing" are now much harder to form and sustain. Consensus-building in international forums is difficult to achieve. It is much easier for opposing actors to be disruptive and to stop initiatives than it is to move these initiatives forward. Disruptions that impede progress at dealing with international issues can occur from nonstate entities as easily as from nation-states. Nation-state legitimacy and authority continue to erode in many regions with the populace identifying more with their religion, ethnicity, race, tribe, class, or other affiliations. These nonstate entities and their impact on national security problems are more evident in the morning headlines every day. As Moisés Naím has argued, obsessing primarily or exclusively about great power rivalries is a red herring that prevents a realistic view of nonstate entities that are dramatically reshaping U.S. national as well as international security interests.[1]

The second driving force is the accelerating pace of, and easier access to, technology mostly being driven by the commercial sector. Fewer technology developments are the exclusive domain of powerful nations and their militaries as occurred during the Cold War.[2] Some of the scientific areas being dominated by nonmilitary research and development are additive manufacturing, including:

- 3D printing
- robotics, autonomy, and artificial intelligence
- energy generation and storage
- synthetic biology
- biotechnology
- nanotechnology
- information technology.

It is not farfetched to imagine open-source design developments and adaptive crowdsourcing by individuals and groups that could allow nonstate entities to "out-innovate" states encumbered by large bureaucracies. It does not take much imagination to conceive of cheap, effective weapons—ranging from the highly disruptive to the absolutely catastrophic—in the hands of individuals or groups with few of the same policy, legal, or ethical impediments for employing them that the U.S. military would have.[3]

The first and second aforementioned drivers are largely empowered by a third one: global communications, such as the Internet and social media, which can have both positive and negative effects. The global communications network accelerates and amplifies ideas and events in unprecedented ways compared to the recent past. This trend is unlikely to subside, and it will continue to slowly undermine state authority, have disproportionate influence on state actions and policies, empower and facilitate groups and movements, and allow technologies and associated design concepts to proliferate worldwide. More individuals and groups will be able to perceive their disadvantaged positions compared to others in the world. Access to other parties with similar grievances will facilitate movements, enable recruiting and radicalization, and support the coordination and execution of terrorist, insurgent, criminal, and other disruptive activities domestically and abroad.[4]

One additional driver that will continue to have a large impact on U.S. national security and global security objectives is the economic power shift from West to East. This "rise of the rest" has diminished the previous dominance of both the United States and the West in terms of economic, political, and security matters. Leading this economic shift from West to East is China, whose emboldened leaders are seeking what they believe to be their rightful place in the world order. No one can be certain if Chinese aspirations to become the new hegemon in East Asia, with a resulting power structure unfavorable to the United States, will actually occur. But few can argue that the relationship between China and the United States is fundamentally important to the interests of both countries and could largely determine future security and stability in the Asia-Pacific region, the vitality of the economies for both nations, and the credibility and influence of American and Chinese power around the world.[5]

These four overarching drivers and other factors will contribute significantly toward diminished global governance trends that could alter U.S. national security perspectives and the future use of the U.S. military in essential ways. First, U.S. influence is being gradually reduced due to its tarnished "brand" from various factors or events including the 2008 global financial crisis, the less than conclusive outcomes in Afghanistan and Iraq, and the perceived U.S. domestic political dysfunction. Many U.S. alliances have weakened without a common threat, causing respective priorities and interests to diverge.[6]

Second, the potential for U.S. retrenchment and disengagement from many of its traditional roles in world affairs is increasing. Much of the American public is frustrated by U.S. global obligations and foreign entanglements that have had questionable effects and return on investment. They see the "American Dream" eroding and want their government to focus more on improving their standards of living rather than engaging in dubious international endeavors.[7]

Third, various global institutions are gradually eroding in influence.[8] These include, but are not limited to, the United Nations, International Monetary Fund, World Trade Organization, and World Bank. A more fragmented or regional world order with reduced U.S. leadership will make it particularly difficult to adequately address critical global challenges. Examples of these possible challenges are nuclear proliferation, international terrorism, large-scale issues related to climate and environmental effects, global financial instability, global economic stagnation, potential worldwide pandemics, global energy availability and associated price volatility, emerging problems in the global commons such as within each of the cyber and space domains, and large-scale regional instabilities or conflicts.

Four Crucial Threat Concerns

The driving forces and trends delineated in the previous section could have significant impact on four crucial threat concerns for the U.S. military in the 21st century. First, increasing global

Airman loads AGM-86B air-cruise launch trainer missile onto B-52H Stratofortress, February 26, 2014, at Minot Air Force Base, North Dakota (U.S. Air Force/Aaron D. Allmon II)

disorder, instabilities, and insecurities could occur with much of the world becoming more dangerous and chaotic.[9] This trend toward a more disorderly world, should it happen, would be largely driven by the rise of malevolent nonstate actors, reduced authority and legitimacy of nation-states in many regions, and decreased ability to provide effective global governance.

A second threat concern would be the further rise of regional hegemons of revisionist powers such as China, Russia, and Iran, whose objectives often clash with U.S. national interests. Should these regional developments occur, particularly as a result of reduced U.S. influence and engagement in those same regions, then the likelihood of adverse regional competition, arms races, and state conflict could be increased.[10]

A third threat concern involves the rise of "super-empowered" individuals and groups capable of levels of violence formerly only within the purview of nations.[11] This ominous threat development is primarily enabled by the increased access to advanced technology by nonstate actors. It represents the dark side of globalization and can take many forms. Imagine individuals or groups operating in garages or small shops employing readily available gene-splicing equipment and genome sequences to synthesize lethal biological agents based on information found in the public domain.[12] Also, consider the possibility of nonstate actors relying on open-source designs and 3D printing to build insect-size drones capable of delivering deadly poisons to assassinate world leaders.[13] Finding these individuals or groups around the globe easily exceeds the law enforcement capabilities in most locales. Thus there is a significant role to be played by multinational intelligence assets, military forces, and other organizations.

The final threat concern would largely complicate the other three. It is a greatly increased level of nuclear proliferation beyond the gradual erosion of the Treaty on Non-Proliferation of Nuclear Weapons that we see today.[14] This proliferation among nations could be enabled if the U.S. nuclear umbrella for key allies was no longer viewed as credible, for example, by perceived U.S. disengagement from their regions. Increasing the number of nuclear nations in East Asia, the Middle East, or elsewhere would correspondingly increase the potential for nuclear accidents, crises, and conflicts in these areas. In addition, proliferation to nonstate actors could be caused by the nexus of nuclear proliferation among nations and the increased access to advanced technology including nuclear weapon designs, nuclear or radiological materials, and related expertise.

Need for a Bifurcated Military Approach

Given these four threat concerns, each of them serious in its own right, how does the U.S. military need to be aligned in order to protect or further U.S. interests in this dangerous future? It needs to adopt a bifurcated approach to deal with both nation-state and nonstate threats. Neither type of threat can be considered a "lesser included case" of the other. They demand significantly different approaches.

To counter nation-state threats posed by countries ranging from near-peer rivals to rogue states, the U.S. military must be prepared to conduct high-tech warfare in harsh antiaccess/area-denial (A2/AD) environments.[15] This would require U.S. forces to have advanced air-missile defenses capable of handling large-capacity adversary attacks to leverage certain U.S. undersea capabilities for asymmetric advantage and to project advanced strike capabilities effectively against a variety of adversary targets. To prevail in high-tech warfare, the military must be able to achieve information dominance by protecting its own assets and by countering those of the adversary including in the crucial space domain. Advanced information operations such as electronic warfare, military deception, cyber attacks, and psychological warfare will need to be integrated with kinetic attacks to achieve maximum effects. The military will need to maintain an adequate and coherent nuclear deterrence posture, a topic that has been largely neglected by portions of the national security community since the end of the Cold War.[16] It will also need to be capable of countering ballistic missile nuclear threats from rogue nations such as North Korea, and be prepared to fight in limited nuclear wars if an adversary should make a potentially ill-advised decision to initiate such a conflict.

Increasing access by nations to commercial technologies will likely translate to effective military applications that will significantly close the gap with the U.S. military.[17] In the future, U.S. ground forces cannot count on air superiority due to advanced missiles and other airborne threats, or the ready availability of satellite communications (SATCOM) and GPS, or being able to conduct operations in strictly non–weapons of mass destruction (WMD) environments. This means that gaining access to areas of operation, conducting expeditionary maneuvers, and defending ground units could prove much more challenging than it has been in recent conflicts. Similarly, U.S. maritime forces cannot count on air superiority, control of the undersea environment due to advanced adversary submarines and other undersea weaponry, or ready access to SATCOM and GPS. As a result, defense of maritime forces and power projection by those same forces could be much more difficult than in the recent past. In future conflicts U.S. air and space forces cannot count on air and space superiority due to advanced integrated air defenses and effective kinetic and nonkinetic antisatellite techniques of their opponents. This means that conducting strikes, close air support, and other missions could be much more challenging than in recent history. Despite these challenges, the United States should not overprepare and overinvest against nation-state opponents at the cost of being ill-prepared for conflicts or contingencies involving nonstate actors.

To counter nonstate threats, including potential super-empowered individuals and groups of terrorists, insurgents, criminals, and other bad actors, significant U.S. military resources and capabilities will need to be developed. This means continuing counterterrorism, including efforts to penetrate adversary information and other networks. It could evolve to increased homeland defense roles and capabilities plus key support to various homeland security endeavors such as combating WMD. Furthermore, U.S. forces will have to improve their ability to operate and fight in urban, mountainous, or other demanding environments. The U.S. military must also increase its ability to deal with so-called hybrid warfare situations (for example, those involving surrogate or proxy forces operating below the threshold of war or adversaries employing an innovative mix of low-tech and high-tech weaponry). Finally, the U.S. military needs to upgrade its messaging capabilities to gain crucial support for its irregular operations.

As indicated earlier, the role of the U.S. military in homeland defense is likely to be elevated in the future due to the increased threat from advanced technologies and systems falling into the hands of nonstate adversaries. Examples of these emerging threats include:

- autonomous undersea vehicles or deep submersible vehicles cutting undersea cables[18]
- manned "tourist submarines" or mini-submarines entering a major U.S. harbor and detonating 5 to 10 tons of high explosives under an oil tanker or liquefied natural gas carrier[19]
- a ship-launched torpedo detonating a radiological dispersal device and wreaking havoc on a major port or base[20]
- mobile mines or improvised underwater explosive devices deployed from surface vessels and detonating against various targets transiting to and from U.S. ports[21]
- heavyweight torpedoes deployed from a camouflaged gravity launcher on a merchant ship, homing on the wake signature of a nearby transiting cruise ship, and detonating lethally under thousands of passengers[22]
- a nuclear-tipped cruise missile fired from a merchant ship or from across the U.S. border and targeting a major urban area[23]
- a ballistic missile with an electromagnetic pulse (EMP) warhead fired from a merchant ship off the continental United States and disabling a major portion of the electric grid for weeks to months[24]
- an unmanned aerial system dispensing deadly biological agents over a dense U.S. city.[25]

If these types of threats develop, it may become necessary to divert key DOD assets to provide the needed homeland protection.

Additional Perspectives

In recent history there has been a diminished willingness of states with traditional militaries to make full use of their destructive power due to policy, legal, regulatory, ethical, moral, and other reasons. These constraints will only be compounded in the future for the U.S. military, particularly when dealing with less discriminating nonstate actors and rogue or desperate nations who have access to advanced technologies. For example, certain transnational terrorists would attempt to employ nuclear or radiological weapons against U.S. or

Sailor assigned to USS *Mustin* stands watch in ship's combat information center during Exercise Valiant Shield 2014, which integrates about 18,000 U.S. Navy, Air Force, Army, and Marine Corps personnel, more than 200 aircraft, and 19 surface ships for real-world joint operational experience, September 16, 2014 (U.S. Navy/Declan Barnes)

other civilian populations if they had an opportunity. Some adversary nation-state militaries, if losing to the United States in a conventional conflict and their leadership feared regime change and its very survival, could choose to employ tactical nuclear weapons against U.S. forces. Conversely, current U.S. policy deemphasizes employment of tactical nuclear weapons on the battlefield.[26] Thus the U.S. military could be viewed as a "disadvantaged user" when it comes to tactical nuclear weapons. Similar examples could be provided for chemical and biological weapons.

Another related illustration is in the realm of EMP weapons. Future adversaries may not hesitate to employ EMP against space and terrestrial targets. U.S. policy is to avoid use of these weapons if they would heavily damage civilian infrastructure. Some U.S. adversaries in the future would be equally indiscriminate in employing the following capabilities:

- offensive cyber weapons or physical attacks against critical civilian infrastructure, such as power grids, financial networks, communication networks, and water and food supplies
- electronic warfare jamming against civilian assets such as GPS
- fully autonomous armed robots
- nanotechnology weapons
- biotechnology-enhanced "super-soldiers"
- kinetic weapons in space with the potential to create debris fields that render portions of that domain unusable.

As a possible disadvantaged user in these and other areas, the U.S. military will need to adapt and compensate for utterly ruthless opponents who are relatively unconstrained by rules of engagement, disproportionate effects, and the need to minimize destruction of infrastructure and civilian populations.

As a final note, many national security problems are such that "war is not the ultimate arbiter," as Joseph Nye has so aptly stated.[27] This would include challenges such as those posed by international terrorism, insurgents, organized crime, maritime piracy, natural disasters, large-scale poverty, mass migration, genocide and other widespread human rights abuses, cyber threats, infrastructure attacks, and nuclear proliferation.

Although military power is unlikely to prove decisive by itself, it could provide a crucial underpinning for nonmilitary components of power such as diplomatic, intelligence, economic, financial, informational, and legal measures.

Guiding Principles

So what are some of the guiding principles for DOD that are consistent with achieving a more cohesive and balanced military approach? The first principle is to emphasize fundamentals. An example would be for DOD and other elements of the national security community to place as much focus on the information and cyberspace domain as they have traditionally done for the ground, maritime, air, and space domains. Information operations have always been important in warfare.[28] But dominating the information domain could prove to be the coin of the realm in 21st-century warfare. Another example is for DOD to maintain its technological edge by greater leveraging of commercial developments in many fields,[29] thus avoiding an overreliance on technology developments within the Defense Department unless absolutely necessary.

The second principle is to emphasize prevention. An illustration would be for DOD to give comparable emphasis to peacetime activities designed to deter and prevent conflicts as it has historically given to planning for war if deterrence and prevention measures fail. This would include a revitalization of nuclear deterrence, not so much by increasing capability or capacity, but by clearly articulating its purpose and continued importance.[30] Revitalization would have a three-fold effect: It would boost morale for those in the military assigned to this mission; it would clarify to U.S. allies and partners any limitations on the nuclear umbrella that is being provided to them; and it would also increase the credibility of the U.S. nuclear deterrent to any potential adversaries.

The third principle is to reduce money pits. An example would be for DOD to seriously address its increasing human capital expenditures, which are unsustainable on their current

trajectory.[31] This adverse trend needs to be reversed in a manner that is not detrimental to the viability of the all-volunteer force. On the material side, DOD needs to reduce its focus on maintaining force structures for large, expensive traditional platforms or systems if they require significantly increased levels of protection or have decreased overall utility against key portions of the emerging threat spectrum.[32]

The fourth principle is to be selective and prioritize. An illustration would be to make only large military resource commitments and expenditures (people, equipment, funding) in areas that clearly involve either vital or very important U.S. national interests.[33] A corollary for the U.S. Government and DOD is to stop attempting to do more with less. This does not work. It is necessary, in fact, to make hard choices by setting priorities that ultimately will help to prevent stretching U.S. military forces too thin. Finally, the U.S. Government and its military must develop effective strategies for each of the long-term national security challenges to which they are committed. Correspondingly, as Mike Vickers stated in recent Senate testimony, the military needs "to identify a decisive element that confers enduring advantage, and then to focus actions and resources on it."[34]

The fifth principle is to avoid tunnel vision. DOD is focusing strongly on countering A2/AD threats posed by certain militaries in key regions such as Europe, the Middle East, and the Western Pacific. As important as this is, it should not be done to such a degree that it is at the expense of dealing with other more likely threats and challenges.[35] For example, irregular warfare and counterterrorism efforts by the military Services against nonstate actors will need to increase to ensure sufficient preparedness against the proliferation of super-empowered individuals and groups, which some believe are just over the horizon. Also, despite contrary strategic guidance released by DOD in January 2012, it is imperative that the U.S. military maintain the capability to conduct counterinsurgency and stability operations of various scales.[36] In the future the joint force can expect to encounter guerrilla forces, including in challenging urban environments. This could occur while either coming to the aid of an ally or partner nation or while attempting to maintain adequate security and order in the aftermath of a conflict that the U.S. military and its allies have just won.

The final principle is to be prepared for out-of-the-box situations. As an illustration, the U.S. Government, with key contributions from DOD, will need to counter challenging asymmetric approaches by potential nation-state adversaries. These include:

- financial attacks
- economic and trade destabilization measures
- sabotage or bombings
- assassinations
- extortion, intimidation, or political coercion
- cyber warfare
- psychological warfare and propaganda
- various gray zone or hybrid warfare approaches conducted through surrogates or other means.[37]

A second illustration is the need for the U.S. military to develop adequate mitigation measures against adversaries employing advanced technologies in which the United States could find itself as a disadvantaged user. This includes resolving policy issues regarding the U.S. military employing systems or weaponry that rely on advances in robotics and artificial intelligence, cyber warfare, directed energy, nanotechnology, synthetic biology, genetic engineering, biotechnology, and other potentially controversial areas.[38] Finally, the U.S. Government, including DOD, will need to dramatically increase its participation in public-private partnerships in order to provide protection against out-of-the-box threats to the homeland.[39] Without these partnerships it is difficult to imagine how sufficient levels of cyber security, bio security, nuclear or radiological security, EMP security, financial security, and energy and power grid security would be achievable.

Conclusion

The primary objective for the U.S. military in a highly constrained budget environment should not be to achieve at all costs a decisive win in a major war against a near-peer rival by dominating that adversary in all warfighting domains. That objective would be extremely resource intensive and technically challenging; it would also consume large portions of future military budgets at the expense of countering other threats that also deserve significant resources and attention.[40] Additionally, a truly decisive win against the conventional forces of a major power could inadvertently escalate that conflict to a nuclear war.[41]

On the contrary, the primary objectives for the U.S. military should be to support efforts to deter adversaries and prevent a major power war as well as other types of conflicts from occurring; if a conflict does occur and is in U.S. national interests, then to help win it in terms of reaching a successful and sustainable political outcome, which may or may not involve a decisive win by the military; and to effectively contribute to mitigating a variety of global security challenges, including those posed by nefarious nonstate actors, by achieving successful outcomes as part of an overall team composed of other U.S. agencies, partner nations, and organizations. Hopefully this set of objectives for the U.S. military would be more affordable, more technically achievable, less likely to result in nuclear escalation, and better able to address a broad set of security challenges.

A properly designed, bifurcated military approach that is employed effectively in coordination with other components of national and international power would support these objectives. Focusing on major power wars and treating other national security challenges as lesser included cases, however, would not. U.S. decisionmakers in charge of developing an effective military approach to counter the emergent threats outlined herein need to choose wisely—U.S. national security and global international security in the 21st century could depend on it. **JFQ**

Notes

[1] Moisés Naím, *The End of Power: From Boardrooms to Battlefields and Churches to States, Why Being in Charge Isn't What It Used to Be* (New York: Basic Books, 2013), 157, 221–224, 235–236.

[2] William J. Lynn III and James Stavridis, foreword to *Creative Disruption: Technology, Strategy and the Future of the Global Defense Industry*, by Ben FitzGerald and Kelley Sayler (Washington, DC: Center for a New American Security [CNAS], June 2014), available at <www.cnas.org/sites/default/files/publications-pdf/CNAS_FutureDefenseIndustry_FitzGeraldSayler.pdf>.

[3] T.X. Hammes, "Cheap Technology Will Challenge U.S. Tactical Dominance," *Joint Force Quarterly* 81 (2nd Quarter 2016), 76–85.

[4] Eric Schmidt and Jared Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business* (New York: Knopf, 2013), 3–5, 34–36, 73, 92, 121–128, 151–156, 165, 178.

[5] Robert Haddick, *Fire on the Water: China, America, and the Future of the Pacific* (Annapolis, MD: Naval Institute Press, 2014), 206.

[6] Zbigniew Brzezinski, *Strategic Vision: America and the Crisis of Global Power* (New York: Basic Books, 2012), 44–46, 53, 67–74, 126, 173.

[7] Elbridge Colby and Paul Lettow, "Have We Hit Peak America? The Sources of U.S. Power and the Path to National Renaissance," *Foreign Policy*, July/August 2014, 54–63, available at <http://foreignpolicy.com/2014/07/03/have-we-hit-peak-america/>.

[8] Colin I. Bradford, Jr., and Johannes F. Linn, *Reform of Global Governance: Priorities for Action*, Policy Brief #163 (Washington, DC: Brookings Institution, October 2007), available at <www.brookings.edu/research/papers/2007/10/global-governance>.

[9] Randall Schweller, *Maxwell's Demon and the Golden Apple: Global Discord in the New Millennium* (Baltimore: The Johns Hopkins University Press, 2014), 41–43, 47, 111, 120–121.

[10] Bret Stephens, *America in Retreat: The New Isolationism and the Coming Global Disorder* (New York: Sentinel, 2014), 133–134, 143, 152–167, 180, 185–206, 228.

[11] John Sutherland, *iGuerilla: Reshaping the Face of War in the 21st Century* (Palisades, NY: History Publishing Company, 2015), 51, 63–65, 183–187.

[12] Benjamin Wittes and Gabriella Blum, *The Future of Violence: Robots and Germs, Hackers and Drones* (New York: Basic Books, 2015), 17–18, 24–28.

[13] Ibid., 33–34, 45, 261.

[14] Henry D. Sokolski, *Underestimated: Our Not So Peaceful Nuclear Future* (Arlington, VA: Nonproliferation Policy Education Center, November 2015), 52–56, 78–88, 93–96, 120–121.

[15] *Joint Operational Access Concept (JOAC), Version 1.0* (Washington, DC: Department of Defense, January 17, 2012), 9–16, available at <www.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf>.

[16] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, *Report of the Defense Science Board Task Force on Nuclear Deterrence Skills* (Washington, DC: Department of Defense, September 11, 2008), 1, 5, 8, 13–16, 46, 68–69, available at <www.acq.osd.mil/dsb/reports/ADA487983.pdf>.

[17] Ben FitzGerald and Kelley Sayler, *Creative Disruption: Technology, Strategy and the Future of the Global Defense Industry* (Washington, DC: CNAS, June 2014), 7, 8, 14, 19–20, 25.

[18] James Stavridis, "A New Cold War Deep Under the Sea?" *Huffington Post*, October 28, 2015, available at <www.huffingtonpost.com/admiral-jim-stavridis-ret/new-cold-war-under-the-sea_b_8402020.html>.

[19] John R. Benedict, Jr., "The Unraveling and Revitalization of U.S. Navy Antisubmarine Warfare," *Naval War College Review* 58, no. 2 (Spring 2005), 103–104.

[20] Jeffrey Lewis, "Putin's Doomsday Machine," *Foreign Policy*, November 12, 2015, available at <http://foreignpolicy.com/2015/11/12/putins-doomsday-machine-nuclear-weapon-us-russia>.

[21] Scott C. Truver, "Mines and Underwater IEDs in U.S. Ports and Waterways: Context, Threats, Challenges, and Solutions," *Naval War College Review* 61, no. 1 (Winter 2008), 106–109.

[22] "The Ongoing Threat to Cruise Ships," *Stratfor.com*, December 14, 2005, available at <www.stratfor.com/analysis/ongoing-threat-cruise-ships>.

[23] "Iran's Cruise Missile Threat and Merchant Ships?" *EagleSpeak*, March 27, 2005, available at <www.eaglespeak.us/2005/03/irans-cruise-missile-threat-and.html>.

[24] Robert K. Ackerman, "Asymmetric Missile Threats Loom on Horizon," *Signal*, October 2005, available at <www.afcea.org/content/?q=asymmetric-missile-threats-loom-horizon>.

[25] Eugene Miasnikov, *Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects* (Moscow: Center for Arms Control, Energy, and Environmental Studies at the Moscow Institute of Physics and Technology, March 2005), 3–9, available at <www.armscontrol.ru/UAV/UAV-report.pdf>.

[26] Amy F. Woolf, *Nonstrategic Nuclear Weapons*, RL32572 (Washington, DC: Congressional Research Service, March 23, 2016), 13–16, available at <www.fas.org/sgp/crs/nuke/RL32572.pdf>.

[27] Joseph S. Nye, Jr., *The Future of Power* (New York: PublicAffairs, 2011), 9.

[28] Leigh Armistead, ed., *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, DC: Brassey's, Inc., 2004), 9, 13–14, 231–233.

[29] FitzGerald and Sayler, 6, 9–10, 16–17, 19, 34–35.

[30] Larry D. Welch and John C. Harvey, Jr., *Independent Review of the Department of Defense Nuclear Enterprise* (Washington, DC: Department of Defense, June 2, 2014), 5–7, 10, 18, available at <www.defense.gov/Portals/1/Documents/pubs/Independent-Nuclear-Enterprise-Review-Report-30-June-2014.pdf>.

[31] Colby and Lettow, 56–58.

[32] Andrew F. Krepinevich, Jr., "The Pentagon's Wasting Assets: The Eroding Foundations of American Power," *Foreign Affairs*, July/August 2009, 18–19.

[33] Jerry Hendrix, *Avoiding Trivia: A Strategy for Sustainment and Financial Security*, Strategic Voices Series (Washington, DC: CNAS, February 2015), 19, 22–23, available at <www.cnas.org/sites/default/files/publications-pdf/CNAS%20Avoiding%20Trivia_final_for%20web.pdf>.

[34] Senate Armed Services Committee, *Improving the Pentagon's Development of Policy, Strategy and Plans*, Testimony of Michael G. Vickers, December 8, 2015, 3–4, available at <www.armed-services.senate.gov/imo/media/doc/Vickers_12-08-15.pdf>.

[35] Robert M. Gates, "A Balanced Strategy: Reprogramming the Pentagon for a New Age," *Foreign Affairs*, January/February 2009, 29–30, 36.

[36] Michael E. O'Hanlon, *The Future of Land Warfare* (Washington, DC: Brookings Institution Press, 2015), 122–125, 138–144, 164–165.

[37] Bill Flynt, "Threat Kingdom," *Military Review* 80, no. 4 (July/August 2000), 17–21.

[38] James Kadtke and Linton Wells II, *Policy Challenges of Accelerating Technological Change: Security Policy and Strategy Implications of Parallel Scientific Revolutions*, Defense and Technology Paper 106 (Washington, DC: Center for Technology and National Security Policy, September 2014), 1, 3, 7–10, 23–30, available at <http://ctnsp.dodlive.mil/files/2014/09/DTP106.pdf>.

[39] Nathan E. Busch and Austen D. Givens, "Public-Private Partnerships in Homeland Security: Opportunities and Challenges," *Homeland Security Affairs*, October 2012, available at <www.hsaj.org/articles/233>.

[40] *Joint Operational Access Concept (JOAC), Version 1.0,* 37–38.

[41] Hugh White, "The New Nuclear War Threat in U.S.-China Ties," *The Straits Times* (Singapore), October 27, 2015, available at <www.straitstimes.com/opinion/the-new-nuclear-war-threat-in-us-china-ties>.