

Understanding Tomorrow Begins Today: The Operational Environment Through 2035

The Operational Environment provides opportunities and challenges

The Operational Environment (OE) is a combination of conditions and variables that impact a commander's decision-making process and his/her ability to employ capabilities. The factors that define a given OE stretch across the Diplomatic, Information, Military, and Economic (DIME) spheres and form the broad setting in which the Army and any of its units, along with its joint and combined partners, conduct operations. Our ability to conceptualize and understand the OE and its lattice-work of variables – the political, military, economic, social, information, infrastructure, physical terrain, and time factors (PMESII-TT) – allows us to not only conceptualize, plan, and train for the types of missions we will face in the near-term, but also to explore the types of capabilities and processes we will need to develop and/or adopt to contend with the threats we will face in the future. Our analysis of the OE indicates that key potential adversaries are focusing on developing capabilities and employing hybrid strategies that will provide direct challenges to Army and Joint and Combined forces.

The OEs of today and the future will be marked by instability. This instability will manifest itself in evolving geopolitics, resurgent nationalism, changing demographics, and unease with the results of globalization creating tension, competition for resources, and challenges to structures, order, and institutions. Instability also will result from the rapid development of technology and the resulting increase in the speed of human interaction, as well as an increasing churn in economic and social spheres. A global populace that is increasingly attuned and sensitive to disparities in economic resources and the diffusion of social influence will lead to further challenges to the status quo and lead to system rattling events like the Arab Spring, the Color Revolutions in Eastern Europe, the Greek monetary crisis, and BREXIT. Also, the world order will evolve with rising nations challenging the post-Cold War dominance of the US-led Western system. New territorial conflicts will arise in places like the South China Sea, compelling us to seek new partnerships and alliances, while climate change and geopolitical competition will open up whole new theaters of operation, such as in the Arctic.

The combination of this instability with the dizzying advances being made in technology and the increased velocity of human interaction means that the OE will present an array of threats that will be lethal and multi-domain (land, sea, air, space, and cyber.) Our adversaries will hide in and among populations and in complex terrain, and endeavor to mitigate many of our own traditional technological advantages and force us to operate with degraded capabilities. They will adopt hybrid strategies that take advantage of a range of capabilities that deny us a conventional force-on-force fight. They will use proxy forces that provide plausible deniability, yet directly allow them to not only shape the battlespace, but even achieve their objectives without risking a wider conflict. Similarly, they also may choose to work with, sponsor, or support terrorist or criminal entities to achieve a similar end. Irregular operations, often in concert with proxies, terrorist, or criminal activities, operating within a "gray zone"¹ short of war will challenge our ability to come to grips with the enemy and perhaps present an unfavorable cost-benefit equation to our political leaders. Our adversaries will rely on strategic capabilities, such as weapons of mass destruction, information operations, and direct cyber-attacks

¹ The "gray zone" is a conceptual space between peace and war, occurring when actors purposefully use multiple elements of power to achieve political-security objectives with activities that cloud attribution and exceed the threshold of ordinary competition, yet fall below the level of large-scale directly military conflict, and threaten US and allied interests by challenging, undermining, or violating international customs norms, or laws.

designed to give us pause in responding to their actions and provide them the strategic space they need to operate. Finally, they will develop conventional force structures capable of providing anti-access and area denial capabilities designed to keep us from entering forces into a battle space, or at a minimum, provide an operational barrier that we will have to spend time and resources to breach. When considered together with the likelihood that our adversaries initially will choose the time and place of the fight, the Army will be faced with the potential of being overmatched in terms of capabilities and out of balance and position in terms of deployment and timing.

We will face thinking, adaptive adversaries

The United States under these conditions will have to contend with the emergence of potential near-peer rivals, well-positioned regional adversaries, increasingly capable and dangerous ideologically-driven terrorist groups, as well as sophisticated and ruthless international criminal syndicates. These adversaries will employ a combination of capabilities that blend traditional terrorism and criminal activities with those once thought only to be within reach of nation-states to drive their own agendas, will remain an enduring threat.

The nation-state adversaries that will challenge us over this time period can be divided into several categories. At the high end will be the **near-peer competitor**, a nuclear-armed state whose strategic forces, conventional military capabilities, and ability to project power approach those of the United States. Although we currently do not face a near-peer competitor, both Russia and China could approach this status in the mid-to-long term². **Nuclear-armed regional powers** are the second type of threat. These states maintain capabilities in all domains and can project power regionally, both conventionally and through the use of surrogates. Their ultimate trump card is a nuclear umbrella, which can be projected out to the intermediate- or even intercontinental-range. Russia, China, and North Korea fit this bill today, and Iran could become such a nation over the mid-to-long term. A third type of threat is the **non-nuclear regional hegemon**, which possesses well-equipped militaries capable of operating across all domains. Although lacking a nuclear deterrent, these states can find other ways to build a deterrent capability, such as developing unique irregular capabilities, cyber capabilities, or other weapons of mass destruction. Iran currently fits this archetype. Non-state actors, such as **ideologically-driven terrorist groups** and **international criminal syndicates** also will take advantage of some of the same factors that nation-states have considered, but will match them with a willingness to rely on other, non-conventional capabilities to achieve their own objectives.

- Russia can be considered our “pacing threat,” and arguably is the most capable of our potential adversaries. Although not yet a true equal to a joint US military force, the Russian military has made considerable progress in reviving its capabilities to wage modern war, incorporating into their operational practices lessons learned from Dagestan, Chechnya, the Crimea, Ukraine, and Syria. Russia is working on a new approach to warfare which combines the use of military force with a broader set of national policy tools³. It has combined this approach – termed Russian New Generation Warfare – with a significant

² For the purposes of this paper, the near-term may be considered the period 2017- through 2022, the mid-term, 2022 through 2027, and the long-term 2027 through 2035.

³ Kristin Ven Bruusgaard, “Crimea and Russia’s Strategic Overhaul,” *The US Army War College Quarterly: Parameters*, Autumn 2014, http://strategicstudiesinstitute.army.mil/pubs/parameters/Issues/Autumn_2014/11_BruusgaardKristin_Crimea%20and%20Russia's%20Strategic%20Overhaul.pdf.

- military modernization program, and unveiled new capabilities in Crimea, Ukraine, and Syria, including the use of proxies – the “little green men” – unmanned and robotic systems, and precision strike weapons.^{4 5} It also has worked on developing other capabilities, including airborne forces, chemical and biological weapons, and a sophisticated cyber capability, that could be used in a hybrid strategy against the United States.⁶ Finally, Moscow has a robust defense research and development program, focusing on developing and incorporating new technologies – such as robotics, unmanned systems, and range of information technology advances – into their military force structure.
- China also is rapidly modernizing its armed forces and considering new approaches to warfare. Beijing’s rapid development, fueled by heavy investment, a relatively strong economy, industrial espionage, and desire to build military power that will match its perceived place as a “great power,” means that China could surpass Russia in the mid-to-long-term as our most capable threat. China’s main areas of focus have been in developing anti-access and area denial capabilities, naval forces, ballistic missiles, and a formidable proficiency in cyber and space operations⁷. It has been expanding its reach away from its shores and out to contested islands in the South and East China Seas – the Senkaku/Diaoyu, Spratly and Paracel Islands, as well as Scarborough Shoal – which means that an increasing number of South East Asian littoral states, such as Thailand, Malaysia, Singapore, Brunei Indonesia, the Philippines, and Vietnam, increasingly could look to regional security partnerships to check Chinese expansion⁸.
 - Although clearly not on the same level as Russia or China, North Korea’s enigmatic political leadership, its large, but outdated military, matched with a relatively sophisticated ballistic missile force and a nuclear capability make it a significant regional threat for the United States through at least the mid-term of this analysis⁹. North Korea’s economic situation remains dire, but the regime’s ability to focus its resources on the military and security apparatuses at the expense of welfare of its population means that it may remain a credible

⁴ Johns Hopkins University-APL, *Little Green Men: A Primer on Modern Russian Unconventional Warfare 2013-2014, 2015*, http://www.jhuapl.edu/ourwork/nsa/papers/ARIS_LittleGreenMen.pdf.

⁵ Valery Gerasimov, “The Value of Science Is the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations,” *Military Review*, January-February 2016, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.

⁶ Johns Hopkins University-APL, *Little Green Men: A Primer on Modern Russian Unconventional Warfare 2013-2014, 2015*, http://www.jhuapl.edu/ourwork/nsa/papers/ARIS_LittleGreenMen.pdf.

⁷ Anthony Cordesman with Joseph Kendall, *Chinese Strategy and Military Modernization in 2016: A Comparative Analysis*, CSIS: Washington, DC: December 5, 2016, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/161208_Chinese_Strategy_Military_Modernization_2016.pdf.

⁸ Richard A. Bitzinger, *Alliance Requirements Roadmap Series: Third Offset Strategy and Chinese A2/AD Capabilities*, Center for a New American Security, May 2016, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Third-Offset-Strategy-and-Chinese-A2-AD-Capabilities_FINAL.pdf

⁹ Office of the Secretary of Defense, “Report to Congress: Military and Security Developments Involving the Democratic People’s Republic of Korea,” January 5, 2016, https://www.defense.gov/Portals/1/Documents/pubs/Military_and_Security_Developments_Involving_the_Democratic_Peoples_Republic_of_Korea_2015.PDF.

regional threat, with a nuclear capability that may reach at least part of the Continental United States¹⁰.

- Iran for at least the near- to perhaps the mid-term of this assessment represents a non-nuclear regional hegemon. It maintains hegemonic ambitions rooted in its culture, history, and traditions, and since its 1979 revolution, has sought to expand its influence and its Shia form of Islam across the Middle East. In many ways, Iran helped pioneer some of the hybrid strategies, such as the use of proxies and asymmetric conflict, which have proven successful on the battlefields of Lebanon, Iraq, and Syria^{11,12}. It also has a well-known civilian nuclear program that could in the mid-to-long-term transition to a military nuclear capability, and has attempted to modernize its own anti-access/area denial capabilities in the Strait of Hormuz region.
- The most capable of the non-state actors today and through the mid-term will be ideologically-driven international terrorist organizations, such as ISIS, al-Qa'ida, or Lebanese Hizballah, who are capable of targeting US interests at home and abroad. A separate category of non-state actor, international criminal syndicates, create further complications, as their capabilities and interests span international boundaries. They ruthlessly intimidate or eliminate their rivals, and even directly challenge governments, as we have seen in Mexico, or previously in Colombia. Both terrorists and criminals may partner with, or accept the support of nation states to acquire advanced weapons, take advantage of the availability of commercial technologies, develop their own unique capabilities, and deftly use social media and cyber capabilities to wage their own information operations. Further, they may often hide and operate within an underdeveloped, or under-governed locale, or even within a failing or failed state, and often within complex urban environments.

Understanding the OE is the first step in maintaining multi-domain dominance

The key to prevailing under the conditions presented in the OE out to 2035 is to take better advantage of its factors, variables, and realities than do our adversaries. Although the nature of war is a historical constant, its character and means have, and will, continue to evolve. The potential adversaries noted above already are researching, adapting, and in some cases adopting new technologies, like robotics, unmanned systems, three-dimensional printing, advanced sensors, anti-satellite and other space capabilities, and whole suites of capabilities within the cyber realm. Coupled with the advantage of time, distance, and space, we will face adversaries who can overmatch our capabilities, and selectively out-gun, out-range, and out-protect our potentially outdated and out of position forces. We will need to work with our traditional allies and forge new partnerships to mitigate or eliminate our adversaries' time, space, and distance advantages, while developing new capabilities, force structures,

¹⁰ OSD, "Report to Congress: DPRK," and Mike Wall, "North Korea's Missile Threats to US May not be Empty for Long," *Space.com*, February 13, 2017, <http://www.space.com/35681-north-korea-intercontinental-ballistic-missiles-threat.html>

¹¹ GEN Lloyd J. Austin III, "Statement of General Lloyd J. Austin III, Commander U.S. Central Command Before the Senate Armed Services Committee on the Posture of U.S. Central Command," March 8, 2016, http://www.armed-services.senate.gov/imo/media/doc/Austin_03-08-16.pdf.

¹² Dexter Filkins, "The Shadow Commander," *The New Yorker*, September 30, 2013, <http://www.newyorker.com/magazine/2013/09/30/the-shadow-commander>.

and doctrine which allow us to maintain our dominance and overmatch against an adversary in a hybrid fight, perhaps in a gray zone, and arrayed against layered anti-access/area denial capabilities that are replete with new technologies and innovations.

- Such a contest will be increasingly lethal in terms of precision, range of engagement, and destructive power – both focused and widespread.
- It will be waged in all domains, where our best advantage may be our ability to effectively and efficiently synthesize and orchestrate our own power across the ground, air, sea, cyber, and space domains.
- It will occur in and among populations and in complex terrain where we will need to develop capabilities to effectively visualize, integrate information, and target within a highly congested and confused battlespace.
- And it will offer challenges in time, location, and situational awareness which if not mastered, or at least mitigated will compel us to operate with degraded capabilities.

In short, we will need to present our adversaries with multiple dilemmas, perhaps employing elements of hybrid strategies of our own to target our adversaries' critical vulnerabilities, some of which may reside outside the military sphere. Understanding the OE is the critical first step in this process, which in turn will allow us to create the concepts that will lead to the adoption of new doctrine, new capabilities, and new processes that take advantage of advanced technologies and the dramatic increase in the speed of human interaction to adapt faster and to maintain our own ability to overmatch any potential adversary at the point of decision.

About the Authors

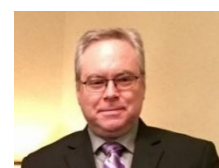
Mr. Ian M. Sullivan, a Defense Intelligence Senior Level (DISL) officer, serves as the Assistant Deputy Chief of Staff, G-2 for ISR and Futures at the US Army Training and Doctrine Command (TRADOC G-2) at Ft. Eustis, VA. He serves in this role as the Senior Advisor for ISR and Futures, where he is responsible for understanding, describing, and assessing the Army's future Operational Environment (OE) in support of leader development, concept development, capability design, and training and readiness.



Mr. Sullivan is a career civilian intelligence officer who has served with the Office of Naval Intelligence, Deputy Chief of Staff, G-2 at the Headquarters, U.S. Army Europe and Seventh Army, and as an Office of the Director of National Intelligence (ODNI) cadre officer at the National Counterterrorism Center, where he served in several leadership positions. He was promoted into the Senior Executive ranks in June 2013 as a member of the ODNI's Senior National Intelligence Service.

Mr. John C. Bauer is the Senior Analyst for TRADOC G-2 ACE Threats at Ft. Leavenworth, KS, where he helps characterize future threats and operational environments in support of US Army capabilities development. He has worked as a strategic defense analyst for academia, industry and government, most recently as one of the architects of US European Command's Deep Futures initiative.

Mr. Eric L. Berry is the Branch Chief for White Sands Missile Range support within the TRADOC G-2's Capabilities Development Scenarios and Studies Directorate, located at Fort Leavenworth, Kansas. Mr. Berry and his team develop and apply high resolution threat and operational environment for a wide range of Army and joint scenario development, studies, and experimentation. He has served in a



variety of intelligence and threat roles for 30 years as a Dept. of Army civilian, and is a retired US Navy Reserve Intelligence Officer with over 30 years of active duty/reserve experience.

Mr. Luke Shabro is the Deputy Director for the U.S. Army TRADOC G-2's Mad Scientist Initiative. Previously he served as U.S. Navy Intelligence Specialist specializing in all-source and geopolitical analysis. He is assigned to TRADOC Headquarters at Ft. Eustis, VA.

