REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-01-2018	Army Science Board Final Report	Feb 2017 - Jan 2018

4. TITLE AND SUBTITLE

The Future Character of Warfare and Required Capabilities

5a. CONTRACT NUMBER
NA

5b. GRANT NUMBER
NA

5c. PROGRAM ELEMENT NUMBER
NA

6. AUTHOR(S)

Michael Macedonia

5d. PROJECT NUMBER
NA

5e. TASK NUMBER
NA

5f. WORK UNIT NUMBER
NA

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Army Science Board
2530 Crystal Dr. Suite 7098
Arlington, VA 22202-3911

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Department of the Army
Office of the Deputy Undersecretary of the Army
Washington, DC 20310-0103

10. SPONSOR/MONITOR'S ACRONYM(S)
HQDA/DUSA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Army Science Board assessed the character of warfare in the 2030-2050 time frame to identify solution strategies for capability development that the Army could initiate in the near-term. The scope of the study included capabilities that would allow the Army to achieve sustainable outcomes in the volatile, uncertain, complex, and ambiguous battlefields of the future. The study team made several findings regarding how imminent changes to the future character of warfare will create both challenges and opportunities for the Army. To address its challenges, the Army will need to recognize and seek solutions for adversaries' increasing accessibility to lethal systems. It will also need to rectify its underinvestment in fielded munitions, talent management, prototyping, experimentation, and simulation. To exploit its opportunities, the Army will need to explore lower risk, higher reward capabilities, i.e., "big bets," that ultimately create and restore operational overmatch.

15. SUBJECT TERMS
Character of Future war; lethality; future operating environment

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Mark S. Swiatek
U	U	U	UU	63	**19b. TELEPHONE NUMBER** *(Include area code)* 7035458657

Reset

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

Army Science Board
Fiscal Year 2017 Study

Character of Future Warfare

Final Report
January 2018

Department of the Army
Office of the Deputy Under Secretary of the Army
Washington, DC 20310-0103

DISCLAIMER:

This report is the product of the Army Science Board (ASB). The ASB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense through the Secretary of the Army and the Chief of Staff, Army. The statements, opinions, conclusions, and recommendations contained in this report are those of the ASB study members and do not necessarily reflect the official position of the United States Army or the Department of Defense.

DEPARTMENT OF THE ARMY
ARMY SCIENCE BOARD
2530 CRYSTAL DRIVE. SUITE 7098
ARLINGTON, VA 22202

March 10, 2018

DUSA-ASB

MEMORANDUM FOR SECRETARY OF THE ARMY

SUBJECT: Final Report of the Army Science Board, "The Character of Future Warfare"

1. I'm pleased to forward the final report of the Army Science Board (ASB) study titled "The Character of Future Warfare." The purpose of the study was to assess the character of warfare in the 2030-2050 timeframe and to identify solution strategies for capability development that the Army could initiate in the near-term. The scope of the study included capabilities that would allow the Army to achieve sustainable outcomes in the volatile, uncertain, complex, and ambiguous battlefields of the future.

2. For this effort, the ASB brought subject matter experts in Computer Science, Telecommunications, Psychology, Structural Dynamics, Strategy, Electrical Engineering, Aerospace Engineering, Chemistry, Physics, Mechanical Engineering, acquisition, and military operations. and a variety of military operations and technologies, as well as former Army and Sister Service leaders. During its seven months together, the study team conducted over twenty visits and interviews among Army and DoD agencies, Federally Funded Research and Development Centers, Academe, and commercial industry.

3. From their work, the study team made several findings regarding how imminent changes to the future character of warfare will create both challenges and opportunities for the Army. To address its challenges, the Army will need to recognize and seek solutions for adversaries' increasing accessibility to lethal systems. It will also need to rectify its underinvestment in fielded munitions, talent management, prototyping, experimentation, and simulation. To exploit its opportunities, the Army will need to explore lower risk, higher reward capabilities, i.e., "big bets," that ultimately create and restore operational overmatch.

4. Based on these findings, the study team recommended the Army develop a Capability Development Strategy to inform decisions on where to make its big bets in areas such as Manned/Unmanned Teaming, commercial network capabilities, lethality, Soldier/team enhancement, cyber, Influence Operations and Electronic Warfare. The study team also recommended the Army increase lethality, embrace commercial and Non-Developmental Item technology acquisition practices for C4ISR, and redesign Army structure for the future operational environment.

5. I hereby endorse the findings and recommendations in this report.

Leonard W. Braverman
Chairman

TABLE OF CONTENTS

APPENDICIES

LIST OF FIGURES

EXECUTIVE SUMMARY

The Army Science Board (ASB) believes the character of future (CFW) warfare will be marked by demographic, social, climatic, economic, technological, and geopolitical trends which will decisively shape the future Strategic Security Environment (SSE). This SSE will be even more complex and lethal than that which confronts the Army today, characterized by shifting alliances among geopolitical actors, persistent conflict with Violent Non-State Actors (VNSA), and the rise of capable and volatile peer and near-peer competitors. Ubiquitous access to technologies by friend and foe alike enable lethality across this entire spectrum. Moreover, U.S. and Allied forces will face asymmetric exploitation of technologies with lethal capabilities by adversaries who don't share the same legal and ethical restraints regarding, for example, weapons of mass destruction (WMD) and robotic and autonomous systems (RAS).

Future SSE trends on the Army Operational Environment (OE) will increase complexity and lethality, and present numerous operational challenges. Two overarching challenges are characterized in the Joint Operating Environment (JOE):[1]

> A range of competitors will confront the United States and its global partners and interests. Contested norms will feature adversaries that credibly challenge the rules and agreements that define the international order. Persistent disorder will involve certain adversaries exploiting the inability of societies to provide functioning, stable, and legitimate governance. Confrontations involving contested norms and persistent disorder are likely to be violent, but also include a degree of competition with a military dimension short of traditional armed conflict.

Drawing upon the JOE, the ASB study team defined five major OE changes that will profoundly influence the Character of Future Warfare (CFW) for the Army and Joint military forces in the 2030-2050 timeframe:

- Conflict Extends to Cognitive Diension – where the competition for will moves from primarily kinetic to increasingly non-kinetic operations.

- Domain Supremacy Contested – the U.S. military is shifting from supremacy in most domains to more contested in all domains.

- Transparent War – a shift from limited, stove-piped command, control, communications, and computer (C4) intelligence, surveillance, and reconnaissance (ISR), to continuous and pervasive, commercial C4ISR.

[1] Joint Operating Environment 2035, The Joint Force in a Contested and Disordered World, 14 July 216.

- Battlespace Reconfiguration – from maneuvering primarily in open terrain and contiguous areas of operation to maneuvering in Dense Urban Areas (DUAs) and dispersed, noncontiguous areas of operation.

- Contested Expeditionary Operations – moving from power projection at will to continuously contested strategic lines of communication, from alert to employment.

To continue operating within this complex but uncertain environment, the Chief of Staff of the Army believes the Army will need to place big bets on modernization. The abundance of options available for new systems and capabilities will further complicate that effort. There's an explosion of potentially disruptive technologies entering exponential growth phases of development (e.g., RAS, AI, commercial ISR and communications, and human enhancement). The Army will need to choose among many viable options while abiding government-imposed constraints in the development, acquisition, deployment, and use of new systems. These constraints include:

- A fiscal environment that restricts research and development (R&D), and procurement funding due to continuing pressures on defense spending by the growth of non-discretionary accounts and national debt.

- The comparatively slow Department of Defense (DoD) acquisition processes that the Army must follow for new programs of record (PORs) as opposed to adversaries' more streamlined processes.

- Asymmetric policy, laws, and regulations between the U.S. and its adversaries regarding the use of lethal capabilities.

The Army needs to establish a Capability Development Strategy (CDS) that addresses these constraints and provides a method to make informed decisions on which of the modernization options to place big bets. Three essential tasks of the CDS should be to:

1. Gain insights into the operational utility of a proposed capability and to explore innovative concepts of operations (CONOPS)/tactics, techniques, and procedures (TTP) that best exploit that capability to provide a well-informed basis for acquisition decisions on the big bets.

2. Accelerate the fielding of limited operational capabilities (LOC) with proven value prior to the formal and agile acquisition of full operational capability (FOC).

3. Build in the ability of new RAS/AI systems to dynamically activate dormant "war reserve" functionality in response to battlefield conditions and changes in the rules of engagement (ROE).

Over the course of its research, the study team developed a series of findings constituting a clear "call to action" for the Army to address the CFW:

- Changes to the CFW create opportunities; exploiting Big Bets will provide overmatch.

- Changes to the Character of Future Warfare (CFW) are inexorable and accelerating, which make maintaining overmatch, without appropriate response, more difficult. Our adversaries are reducing, if not eliminating, our overmatch.

- Easy global access to emerging technologies (Robotic Autonomous Systems (RAS), Cyber, Influence Operations (IO), Artificial Intelligence (AI), and human enhancements) are leveling the playing field, and increasing lethality.

- "We've been here before," (e.g., 1941, 1978):
  - When confronted with an existential threat, the U.S. unified & exploited our technological & entrepreneurial strengths.
  - U.S. Army recognized the value of the individual Soldier resulting in the all-volunteer force.
  - Recognition of new threats (e.g. Israeli 1973 war) motivated Army leadership to respond.

- Even without Allies' recognition of an existential threat, the U.S. will have to make the preponderance of the Allied national security investment.

- Army leadership has recognized the impact of the Ukrainian war yet has not communicated the solutions for our Army to respond to this type threat.

- The Army has underinvested in new, fielded munitions since mid-80's.

- Army lacks Capability Development Strategy across Centers of Excellence to exploit:
  - Innovative and disruptive Training & Talent Management.
  - Operational experimentation & simulation to understand capabilities and to formulate innovative CONOPs.
  - Prototyping to accelerate fielding of limited operational capabilities.

- The all-volunteer force provides the U.S. a clear advantage. The value of individual Soldiers and teams drastically increase as combat capabilities proliferate to our adversaries. Battlespace reconfiguration and transparency argues for smaller, dispersed & trained units.

- Combined and Joint capabilities migrate to lower echelons, with leaders more capable for conflict in all dimensions (physical, information, cognitive).

- The Army has no plan to defeat enemy integrated air defense. Non-developmental Unmanned Aircraft System (UAS), coupled with innovative CONOPs, appears a viable approach to mitigate Integrated Air Defense (IAD) challenge.

- The introduction of ground and air robotic combat vehicles changes both the lethality and survivability parameters.

Key recommendations derived from these findings include the Army implementing the CDS, developing innovative CONOPs to gain overmatch in an era of technological parity, and prioritizing Manned-Unmanned Teaming (MUM-T) investments across successive Programming Objectives Memorandums (POMs). The study team also recommended the Army increase lethality, embrace commercial and Non-Developmental Item (NDI) technology acquisition practices for C4ISR, and redesign the Army for the future OE. Specific investment opportunities for the big bets recommended are:

- MUM-T armed ground robotic vehicles

- Commercial network capability for Army participation in Multi-Domain Battle (MDB)

- Lethality

- Education, training, cadre, facilities, and infrastructure to enhance overmatch in Soldier (enlisted, warrant officer, and officer) and team performance

- Cyber, Influence Operations, and Electronic Warfare (EW) as Army tactical weapons systems

- Leverage DARPA innovation (e.g., Cognitive EW, Swarming UAVs & Offset, Squad-X)

1. INTRODUCTION

In his address at the Association of the United States Army's (AUSA) Eisenhower Luncheon, General Mark A. Milley, the Chief of Staff of the Army (CSA), addressed the Army's current state of readiness and what he saw the Army facing in the years ahead. The CSA outlined the need for the Army to address fundamental changes, as a matter of principle, or prepare to lose the next war. "War tends to slaughter the sacred cows of tradition, of consensus, of group-think and myopia," he said, "and it's better for us to slaughter our sacred cows ourselves, rather than lose a war because we're too hidebound to think the unthinkable."[2]

Specifically, the CSA challenged the Army with three imperatives:[3]

- To **place the big bets**, **the big bets in research and development** and **science and technology**, while simultaneously conducting legitimate and genuine **experiments** with our force designs and our doctrine.

- **Every assumption** we hold, every claim, every assertion, every single one of them **must be challenged**. … Those of us, or those **nation-states that stubbornly cling to the past will lose**. They will lose that war, and they will lose it in a big way.

- **Think of nothing in the past as sacred**, except the concept of victory.

The study team adopted these principles as guidance from the CSA for the conduct of this study. The fundamental shifts that he identified, some of which encompass the changing CFW, tend to expose the Army's response, or lack thereof, to the changing OE.

The study team also adopted a second point made by the CSA, an important distinction between the nature and character of warfare. To summarize, the nature of war is immutable, "the threat of violence, as an extension of politics, to compel the enemy to our will within the fog, friction, and chance of combat." On the other hand, the character of warfare, or the manner in which wars are fought, "changes due to unique geo-political, social, demographic, economic, and technological developments interacting, often unevenly, over time."[4] The team used this distinction in developing its methodology and data gathering plan.

[2] Milley, Gen. Mark A. Address to the AUSA Eisenhower Luncheon, Washington D.C., 4 October 2016. http://wpswps.org/wp-content/uploads/2016/11/20161004_CSA_AUSA_Eisenhower_Transcripts.pdf; p. 15.
[3] Ibid.
[4] Ibid.

1.1 TERMS OF REFERENCE (TOR)

The Commanding General (CG), U.S. Army Training and Doctrine Command (TRADOC) sponsored this study, asking the ASB to assess the character of warfare in the 2030-2050 timeframe. The TOR[5] further states:

> The future operational environment will be characterized by a high potential for instability driven by the diffusion of power and technologies among rising regional states, non-state actors, and increasingly empowered individuals. Adversaries will attempt to apply emerging technologies, diverse organizations, improvised weapons, and weapons of mass destruction to increase battlefield lethality, impede access, and deny the initiative to the U.S. military, contesting it in the air, land, sea, space, and cyberspace military warfighting domains.

To assist the Army in determining how best to address these challenges, CG TRADOC specified six tasks for the study team:

1. Assess and refine the projection of the world environment in 2030-2050 as it affects U.S. Army requirements and capabilities, especially related to the emerging Multi-Domain Battle concept.

2. Assess if there will be fundamental changes in the character of warfare in 2030-2050. What will these changes be, what are the drivers to these changes, and what are the implications to the U.S. Army?

3. Identify the capabilities the U.S. Army must invest in today, divest over time, and recapitalize to fight and win in the complex world of 2030-2050. Are there current U.S. Army capabilities that may not be required in 2030-2050? Are there potentially more effective and/or efficient alternative means of satisfying current requirements?

4. What policy and/or legal constraints (e.g., extending the range of cross-domain fires, conducting cyberspace operations at the tactical level, and employing lethal autonomous systems) need to be addressed in order to enable the Army to operate effectively in the 2030-2050 timeframe?

5. How will the character of war in 2030-2050 challenge American and U.S. Army ethics, morals, and values, notably when adversaries have a fundamentally different moral approach to war, violence, and enhancing human performance?

6. How should the U.S. Army prepare leaders and Soldiers for disaggregated and independent operations in degraded environments, including dense urban areas, in

[5] The TOR is reprinted at Appendix A.

2030-2050? What are the emerging technologies and capabilities that will be decisive in these environments?

1.2 STUDY TEAM, VISITS, AND REFERENCES

The study team selected to address these tasks included ASB members (see Appendix B) with significant technical expertise and experience in a wide range of disciplines, including Computer Science, Telecommunications, Psychology, Structural Dynamics, Strategy, Electrical Engineering, Aerospace Engineering, Chemistry, Physics, Mechanical Engineering, acquisition, and military operations.

During the study, the team conducted over twenty data-gathering visitations (see Appendix C) and interviews with Army agencies, the Office of the Secretary of (OSD), and other Services, think tanks, and commercial companies. The study team also made use of a broad array of earlier studies that describe the future strategic and OE trends out to 2050. Rather than attempt to devise an a-priori, "blank slate" assessment of the character of future warfare, the study team surveyed and synthesized the most important and relevant recent studies, road-mapping, and strategy documents within partner nations, OSD, the Army and the other military services (see Appendix D).

1.3 STUDY LOGIC

The study team worked to identify the most significant current-to-future discontinuities, or "from-to" comparisons, likely to generate significant changes in the future character of warfare Fig. 1.0). These "from-to" discontinuities were collected and logically aggregated into common threads for both the Strategic Security Environment (SSE) and the OE. Analyses of these common threads generated the team's findings and recommendations.

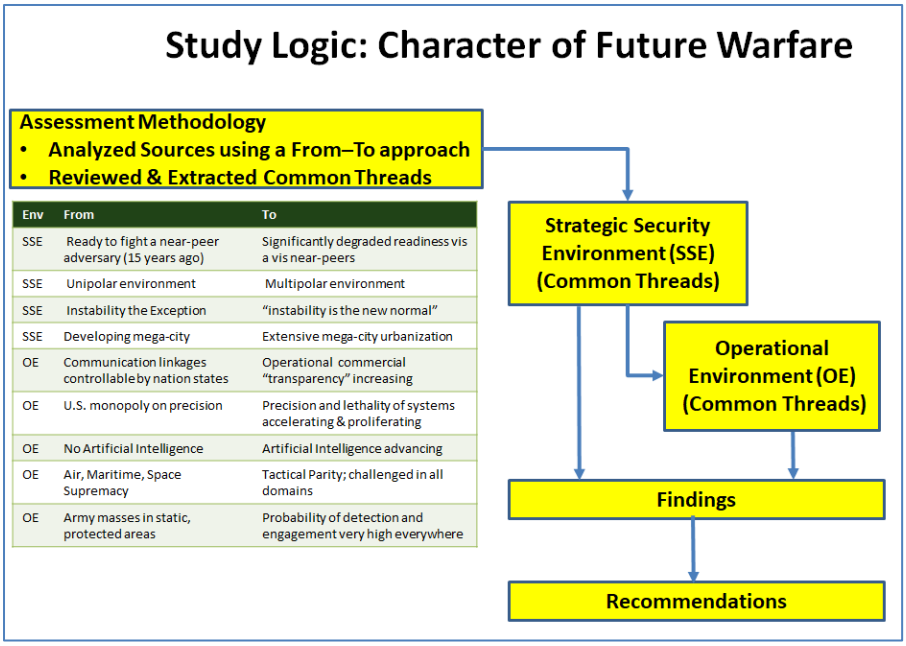


Figure 1.0 Study Logic

2. STRATEGIC SECURITY ENVIRONMENT (SSE)

Man is a deterministic device thrown into a probabilistic universe – Kahneman and Tversky[6]

It's dangerous to attempt to predict what the future will hold between 2030 and 2050 because we're all influenced by the heuristics that we've developed over time. We might build a probable future throughout the next five-year, Future Years Defense Program (FYDP) (Fig. 2.0). But every morning, roughly seven billion people wake up and get a vote regarding how the future will play out. Any prediction beyond five years faces a multitude of factors and greater uncertainty, where an array of possible futures exists.

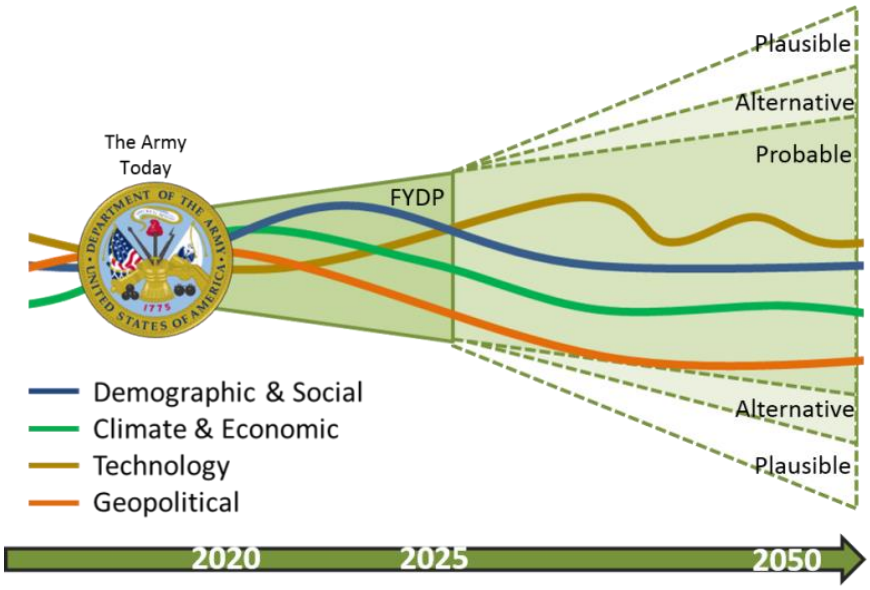


Figure 2.0 The Army of Today Faces a Broad Number of Possible Futures

That said, several people (herein referred to as "futurists") are predicting potential future outcomes, given current global trends and anticipated changes. The study team reviewed a diverse set of samples[7] and from the resulting analysis determined the Strategic Security Environment (SSE) trends that may affect the CFW can be characterized by four, broad categories: (1) demographic and social; (2) climatic and economic; (3) technological; and (4) geopolitical. These trends are multi-faceted, complex, and intertwined on both national and global scales, resulting in multi-variant predictions of potential CFW scenarios.

In each case the team reviewed, the predicted, nonlinear, and rapid progression of affordable technology with widespread availability was anticipated to play a disruptive role in changing the CFW in ways we cannot yet begin to predict. As a result, the team focused the study on identifying key factors producing discontinuities that will most likely impact the future OE for

[6] Michael Lewis, *The Undoing Project: A Friendship That Changed Our Minds*, 2016.
[7] See Appendix D for full list of reports reviewed by the study team.

the U.S. Army. As with any discontinuity, the potential for duality exists, i.e., the potential for both challenges and opportunities, albeit not always of equal importance and/or impact.

2.1 DEMOGRAPHICS AND SOCIAL

The U.S. and other well-developed countries show trends with aging populations and birth rates dropping to historic lows,[8] as affluence grows, and people use their resources to advance their education and lifestyles vice raising children. As the numbers of military-age youth decline within the U.S., its allies and/or coalition partners, recruitment for the countries' armies may become more challenging, with the potential to result in reduced force capability.

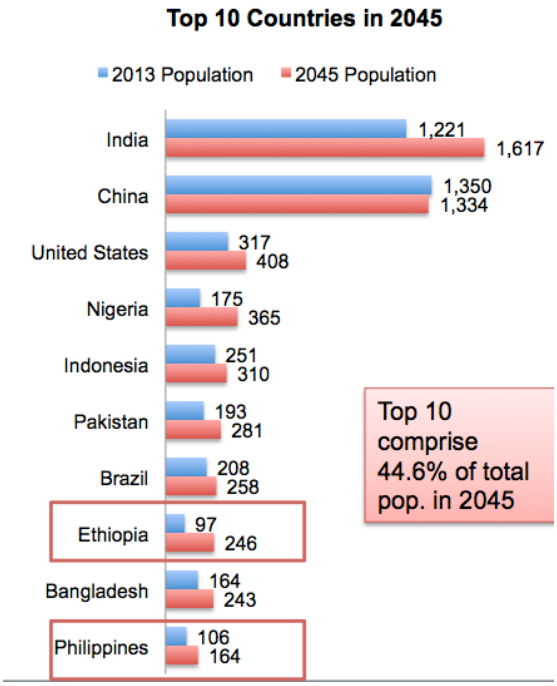


Figure 2.1 Predicted Population Growth 2013-2045 for 10 Countries

Many developing countries have slower declines in birthrate than developed nations (Fig. 2.1) because they haven't realized the benefits of higher standards of living and prosperity. In the future, countries such as Nigeria, Kenya, and Indonesia are predicted to grow large populations of military-age youth. Previous trends demonstrate this change, coupled with economic disparity and high unemployment rates, may result in significant numbers of disenfranchised youth. In turn, this may lead to increased incidents of civil unrest (state- or non-state actors), terrorist-like activities, and or migration by those seeking better standards of living or escaping persecution. The U.S. Army may be called upon to assist allies in addressing civil unrest or providing humanitarian aid to those seeking asylum.

As nations continue to develop from agrarian to more industrial/service economies, futurists predict that people will continue to migrate to urban centers, seeking a better standard of living and resource efficiencies. That trend will result in the acceleration of the development of megacities and dense, urban areas (DUA). As recent history has demonstrated in Mosul, the potential for civil unrest and difficulties in governing DUAs will result in more operational requirements for the Army.

[8] Max Roser and Esteban Ortiz-Ospina (2017) – 'World Population Growth'. *Published online at OurWorldInData.org.* Retrieved from: https://ourworldindata.org/world-population-growth/ [Online Resource].

2.2 CLIMATE AND ECONOMICS

As Thomas Friedman wrote, "The world is flat," thanks to decreasing transportation costs, global business expansion, U.S. corporate tax rates, and increasing access to networks and connectivity. Corporations such as Netflix[9] and Apple[10] will continue to expand internationally (Fig. 2.2), and world trade will continue to intertwine, with China predicted to be the potential leader in world exports by the year 2050[11] (Fig. 2.3).

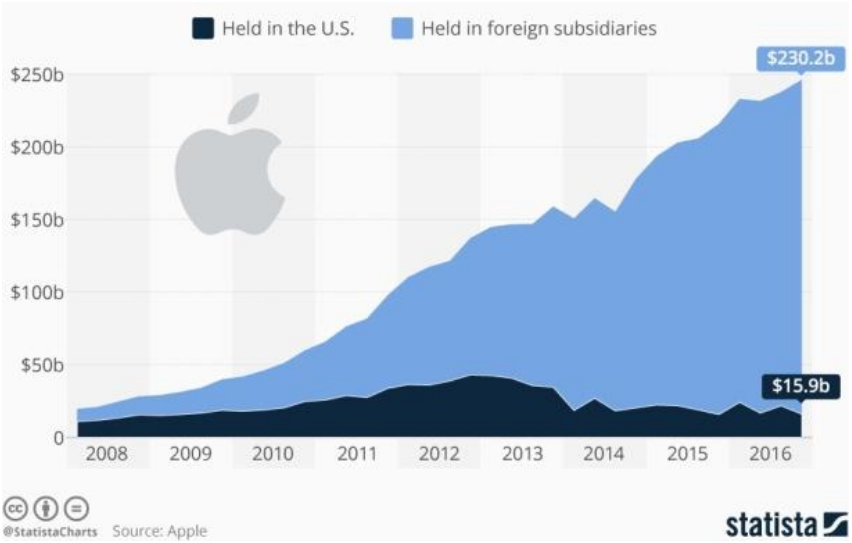


Figure 2.2 Growth in Apple's Cash, Cash Equivalents, and Marketable Securities 2008-2016

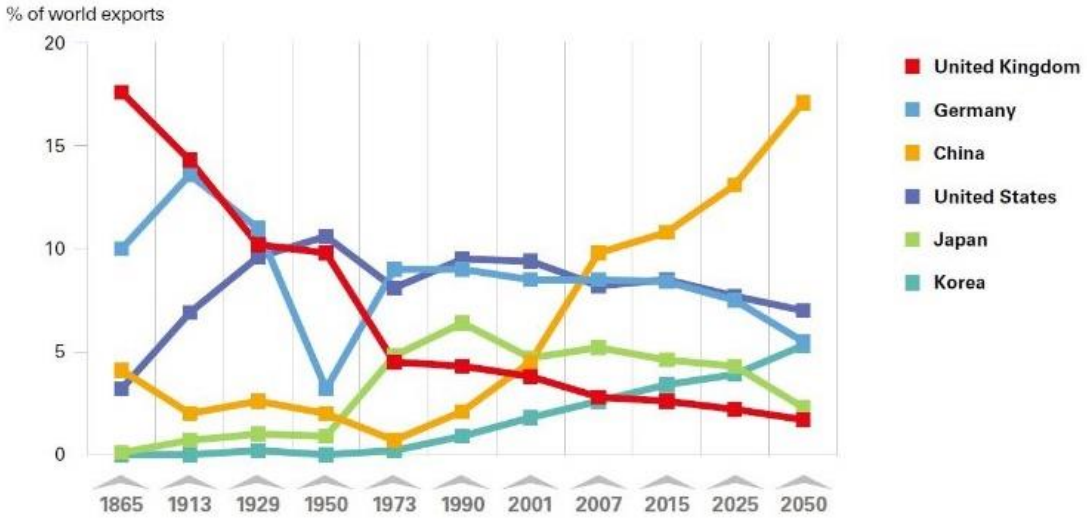


Figure 2.3 Predictions of World Exports for Six Countries

[9] Steel, E., *Netflix nears 100 million subscribers*, New York Times, January 18, 2017.

[10] Mickel, T., *Apple's Cash Hoard Set to Top $250 Billion,* Wall Street Journal, April 30, 2017.

[11] See Justin Paul (2016) The Rise of China: What, When, Where, and Why?, The International Trade Journal, 30:3, 207-222, DOI: 10.1080/08853908.2016.1155513; and https://www.linkedin.com/pulse/trade-winds-685-trillion-future-global-commerce-debra-d-agostino/.

The reduced costs of manufacturing and transporting goods have created an open marketplace for almost anything in the world, helping to raise the standard of living around the world, and serving as a partial economic equalizer for previously disadvantaged populations. They may also grow the economic power of larger state-actors or corporations, shifting today's current economic power status. World trade is predicted to continue to grow in the future, making big winners out of those who can develop the latest technologies first, but those economic advantages may be short-lived if the leading-edge technologies are easily obtained and duplicated.

Corporations are also predicted to continue to grow internationally, influencing global, geopolitical dynamics in unique ways. In the past, U.S. companies provided assistance during humanitarian crises, both domestically and abroad. In the future, corporations may also serve as more involved partners, promoting the positive message of democracy and capitalism.

Futurists also anticipate that climate change will continue to result in increasing temperature variations, increased incidents of extreme weather disruptions, and devastating storms, with the potential to cut or change routine access to essential resources supporting populations (i.e., water, food, and energy).[12] Coupled with increasing populations in less developed areas that don't have the infrastructure to be resilient, the effects of climate change may lead to increased migration to DUAs and/or more civil unrest in nations that aren't well-prepared for the changing dynamic. Such events may further drive instabilities requiring the U.S. Army to get involved, either providing humanitarian aid or helping partner nations stabilize law and order during recovery. In addition, from a military perspective, although climate change may not raise sea levels or temperatures enough to change how the Army may conduct ground force engagement, the Army will need to be prepared to change how essential resources are transported to its forces, given that the typical supply lines and power sources may experience significant disruptions.

2.3 TECHNOLOGY

With the advent of worldwide, high-speed internet access (e.g., OneWeb[13] and SpaceX evolving satellite constellations[14]) and the growth in cell phone usage,[15] global connectivity and the ease with which information moves have accelerated the "flattening of the world." Virtually anyone can purchase inexpensive access to multiple types of information, such as the satellite imagery of a specific location. Increased connectivity also enables almost any entity, from anywhere in the world, to disseminate information, with the potential to produce detrimental effects. The

[12] Bort, R., *How Climate Change's Effect on Agriculture Can Lead to War*. Newsweek, Feb. 17, 2017.
[13] Wyler, G., We All Need Access, One Web, Dec. 19, 2016. Note from Founder and Chairman available at http://oneweb.world/.
[14] Private communication: Briefing by Bryon Hargis, SpaceX Federal Program Manager, July 10, 2017.
[15] https://en.wikipedia.org/wiki/The_World_Is_Flat.

use of social media during the "Arab Spring" uprising[16] and Russia's misinformation campaigns in the Crimea and the Ukraine[17] provide telling examples of the possibility for wreaking havoc in a matter of minutes. Ultimately, cognitive security,[18] which includes the application of AI to detect threats and protect systems, will endure greater and greater risks if the means aren't developed to ensure accuracy and to rapidly debunk false or misleading information.

Although cyber security continues to improve, increasing numbers of hacking incidents, identity thefts, and insider leaks[19] take place, putting individuals, businesses, corporations, governments, and countries at greater risk for loss of intellectual property (IP), trade secrets, financial records, and private/personal information. Spoofing incidents are also on the rise via social media, the hacking of sensor capabilities,[20] and the reporting/relaying of specious news.

There's a very real risk that the U.S. will lose its tactical supremacy, because current, potential adversaries continue to improve their weapons precision and lethality, and weapons technology (e.g., the potential use of lethal RAS[21] capabilities) proliferates unabatedly. The situation is exacerbated by the likelihood that adversaries won't abide by the same codes of conduct or ROE as the U.S. and its allies due to differences in policy, treaties, and legal and ethical frameworks. Thus, it's likely the U.S. will encounter an overmatch scenario resulting from technological parity that's overcome by adversaries willing to maximize the indiscriminate, destructive power of technology. How will the Army respond to the policy and ROE disparities? The study team believes back-up capabilities and processes need to be developed and assessed now, so that they can be dynamically activated when these disparities arise.

Futurists also predict that internet access to weapons technology will continue to reach broader populations, eroding the potential for a U.S. advantage. For example, North Korea[22] has

---

[16] Brown, H., Guskin, E., and Mitchell, A., *The Role of Social Media in the Arab Uprisings,* Pew Research Center, November 28, 2012, Retrieved from: http://www.journalism.org/2012/11/28/role-social-media-arab-uprisings/.

[17] Yun Chee, Foo, *NATO Says it Sees Sharp Rise in Russian Disinformation Since Crimea*, Reuters, February 11. 2017, Retrieved from: http://www.reuters.com/article/us-ukraine-crisis-russia-media-idUSKBN15Q0MG. MacFarquhar, N., *A Powerful Russian Weapon: The Spread of False Stories*, NY Times, August 28, 2016, Retrieved from: https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html. Peterson, N., *In Ukraine, Russia Weaponizes Fake News to Fight a Real War,* March 30, 2017, Retrieved from: http://dailysignal.com/2017/03/30/in-ukraine-russia-weaponizes-fake-news-to-fight-a-real-war/.

[18] Waltzman, Rand, "The Weaponization of Information: The Need for Cognitive Security," document CT-473, Testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity, on April 27, 2017. Available at https://www.rand.org/pubs/testimonies/CT473.html.

[19] Szoldra, P., *This is Everything Edward Snowden Revealed in One Year of Unprecedented Top-Secret Leaks*, Business Insider: Tech Insider, September 16, 2016. Retrieved from: http://www.businessinsider.com/snowden-leaks-timeline-2016-9.

[20] Goward, D., *Mass GPS Spoofing Attack in the Black Sea?*, July 11, 2017. Retrieved from: http://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.

[21] Army Science Board, "Robotic and Autonomous Systems of Systems Architecture" (2017).

[22] Arms Control Association, *Chronology of U.S.-North Korean Nuclear and Missile Diplomacy,* July 2017, Retrieved from: https://www.armscontrol.org/factsheets/dprkchron, and Yun, Byung-se, North Korea and WMD Use: Specific Action is in Order," March 2017, Huffington Post, Retrieved from

benefitted from WMD proliferation, challenging the Army's preparedness for expeditionary maneuvers and response capabilities in a WMD or nuclear environment. From an Army OE perspective, there's a potential for any military, technological advantages to be cut short, because adversaries of all types may gain unprecedented access to disruptive technologies and capabilities. A future challenge will be how to conduct military operations within this rapidly evolving dynamic.

Futurists also predict increased spoofing of all communications, sensing, and operational network capabilities, forcing the Army to operate in an environment flooded with erroneous information. Ultimately, the Army must consider cyber security a priority in tandem with the operational assumption that it won't be able to maintain any new, tactical, technological advantage for long. Thus, the Army must plan to exploit other potential capabilities, including but not limited to AI, human enhancements, and information operations (IO).

The improvement of AI through the 2030-2040s promises to yield new capabilities for the Army. Machines have demonstrated a better ability to make decisions about uncertainties and probabilities than humans. A human's cognitive bandwidth restricts our ability to make decisions as quickly, and humans can use improper heuristics when dealing with decisions in uncertainty. The development of AI will exponentially compress the Observe-Orient-Decide-Act (OODA) decision space, and AI will likely surpass human abilities in all cognitive tasks (Fig. 2.5).[23] Any nation that develops cyborg-like man-machine interfaces will have an advantage, and the Army needs to continue R&D investments in the man-machine AI interface.

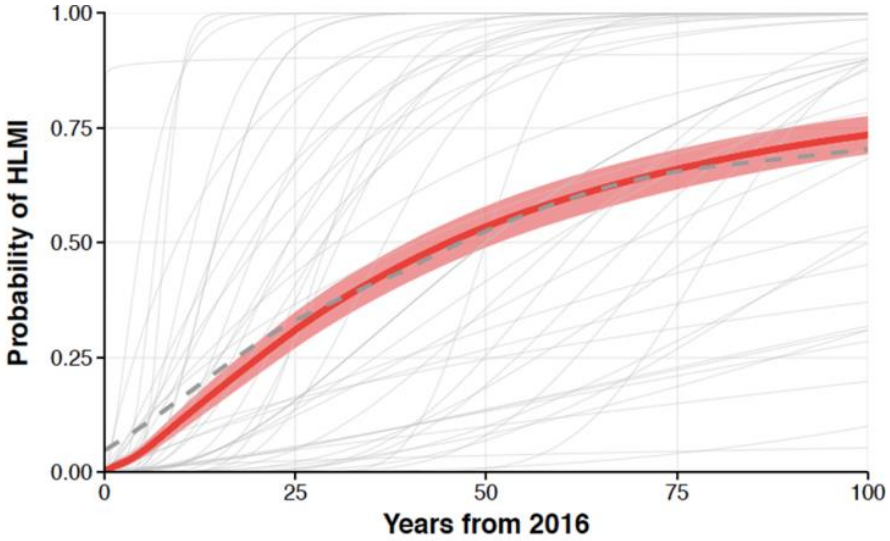


Figure 2.4 Probability of 'High-Level Machine Intelligence' (HLMI) in Future Years[24]

http://www.huffingtonpost.com/entry/north-korea-and-wmd-use-specific-action-is-in-order_us_58bbce7fe4b0fa65b844b461.

[23] Grace, K., Salvatier, J., Dafoe, A., Zhang, B., and Evans, O., *When Will AI Exceed Human Performance: Evidence from AI Experts*, arXiv:1705.08807v2 [cs.AI] 30 May 2017.

[24] Aggregate subjective probability of 'high-level machine intelligence' (HLMI) arrival by future years. Each respondent provided three data points for their forecast and these were fit to the Gamma CDF by least squares to

Beyond more traditional forms of technology (i.e., weapons and machines), the Army will likely face challenges from augmented human combatants fielded by adversaries. The 2016 ASB Solider Enhancement Study[25] outlined opportunities and progress to date for optimization and enhancement technologies in the human physical, cognitive, and psychological domains. As with the employment of certain types of weapons systems, there are cultural, legal, ethical, and moral asymmetries between the U.S. and its potential adversaries that may put the U.S. at a disadvantage on the battlefield. A common and well-documented enhancement technique involves modification using drugs and other biochemical procedures, such as stimulants and psychotropics. The technique has been used by the Germans when they invaded France,[26] by U.S. pilots on long-range missions, and by jihadists fighting for terrorist groups.

More recently, since 2012, Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR) R&D activities have advanced, resulting in thousands of research papers and the start-up of multiple companies in the U.S.[27] China leads the way as the first nation to conduct human trials in terminally ill lung cancer patients. CRISPR technologies hold the promise of a rapid medical countermeasure capability for bacterial and viral infections, as well as for chronic diseases, if successful *in vivo* delivery methods can be demonstrated. On the down side, CRISPR technologies also offer the prospect of unprecedented genetic modifications in humans, flora, and fauna that may be difficult to detect or mitigate.

Finally, adversaries' non-kinetic IO[28,29] will play a more significant role in future environments, with greater impact prior to, during, and after any kinetic engagements. Near-peers such as Russia and China[30] consider IO a key element in influencing local populations and gaining support. For both nations, IO is part of their ongoing operational activity that never ceases. Given U.S. law and military doctrine, the Army will need to consider what changes in national policy and international agreements, if any, it may wish to pursue in the near-term to prepare successfully for maneuvers in non-kinetic, IO environments. More explicitly, the Army may also need procedures that allow for dynamic activation of certain ROEs, given the rapidly evolving character of warfare.

---

produce the grey CDFs. The "Aggregate Forecast" is the mean distribution over all individual CDFs (also called the "mixture" distribution). The confidence interval was generated by bootstrapping (clustering on respondents) and plotting the 95% interval for estimated probabilities at each year. The LOESS curve is a non-parametric regression on all data points.

[25] Army Science Board, "Soldier Enhancement Study" (2017).

[26] Ohler, N., *Blitzed: Drugs in the Third Reich*, Houghton Mifflin Harcourt Publishing, Boston, MA, 2017.

[27] Cohen, J. "How the battle lines over CRISPR were drawn", Science, February 15, 2017.

[28] McClintock, B.H., "Russian Information Warfare: A Reality that Needs a Response", U.S. News and World Report, July 17, 2017, Retrieved from: https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html and https://www.rand.org/topics/information-operations.html.

[29] Fastabend, D., Becker, J. and Gardner, G., "Mad Scientist: The 2050 Cyber Army", November 7, 2016.

[30] Tucker, P. China's Information Warriors Are Growing More Disciplined, Say US Cyber Leaders, Defense One, April 4, 2017, Retrieved from: http://www.defenseone.com/threats/2017/04/chinas-information-warriors-grow-more-disciplined-effective-us-cyber-leaders/136732/.

2.4 GEOPOLITICAL

There's significant overlap among the previous categories regarding factors that affect the geopolitical situation. Futurists predict that competition between state- and non-state actors will continue, and that the U.S. "superpower" supremacy gap will narrow or disappear. China, for example, has been positioning itself to challenge the U.S., and its continued economic growth will further improve its global status.[31] Futurists predict that as development continues, China's central planning model will have to devolve and become more transparent to help keep a lid on corruption and prevent it from causing harm to the economy.[32] However, the Chinese population will continue to age, and total population will decline, as they haven't been able to overcome the lingering effects of the one-child policy.

The potential shifts in global power will also be driven by domestic constraints on U.S. and allies' military budgets and rapid changes in technology, all leading to increased parity between military capabilities.

China and Russia are exploiting these trends to grow their regional power in what they see as declining American supremacy. Currently, the re-establishment of former Soviet Union/Warsaw Pact alliances in Europe and the "One Belt, One Road" (Fig. 2.5) plan in Asia are reshaping economic dependencies that may in turn drive changes in security alliances. "One Belt, One Road" is a series of strategic investments by China, differing from the US approach of using international aid, because China is maintaining ownership in the projects and staying involved in the countries they are investing. Futurists predict that China will continue to use its economic power to influence its neighbors.

More explicitly, futurists anticipate that the military will need to not only identify new procedures and policies, but also develop training that allows the commanding officer to rapidly adapt the OODA process given a rapid turn of events. The Army needs to prepare for these trends by discerning what effects changes in economic dependencies and international security agreements will have for the force.

[31] *While U.S. Retreats, China Gains Ground*, Associated Press, published in Omaha World Herald, July 30, 2017; also *How a Serbian Town Shows China's Global Expansion; US Retreats*, Available at South China Morning Post http://www.scmp.com/news/china/diplomacy-defence/article/2102160/how-serbian-town-shows-chinas-global-expansion-us.

[32] Lam, Willy (4 February 2015). "Growing CCDI Power Brings Questions of Politically-Motivated Purge." The Jamestown Foundation.

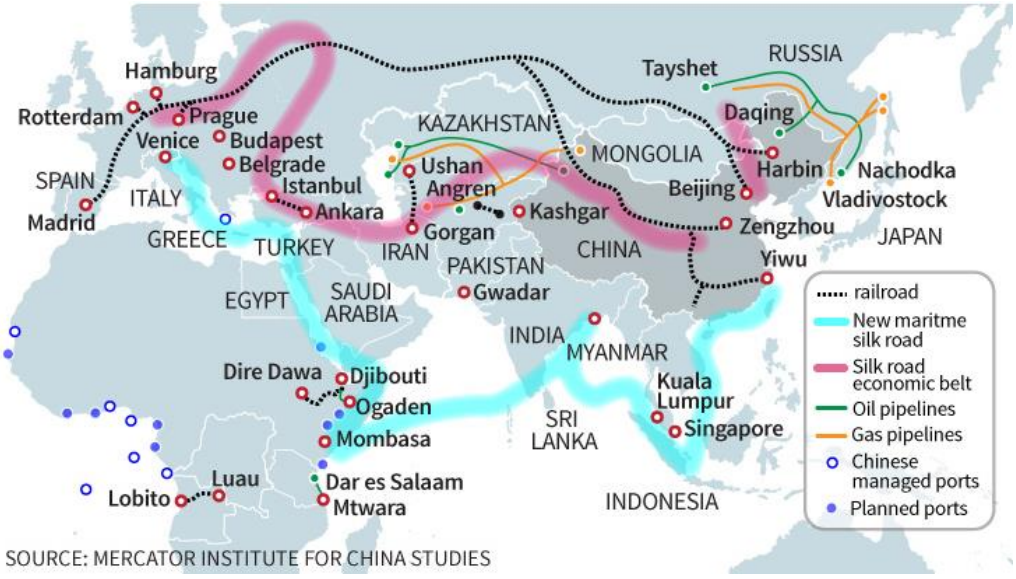


Figure 2.5 Infrastructure Projects in China's Belt and Road Initiative[33]

These trends will play out in any number of potential futures.[34] By 2030, the U.S. is likely to face significant peer threats in Russia and China (despite both having aging populations), increasing potential threats from near-peers in Asia and Africa, and continued threats of violence from non-state actors.

2.5 IMPLICATIONS OF TRENDS IN THE SSE

Understanding the constraints of uncertainty in trying to predict the future, the study team drew from the previous trends five likely consequences that will drive more specific Army and Joint military capabilities in the OE (Fig. 2.6):

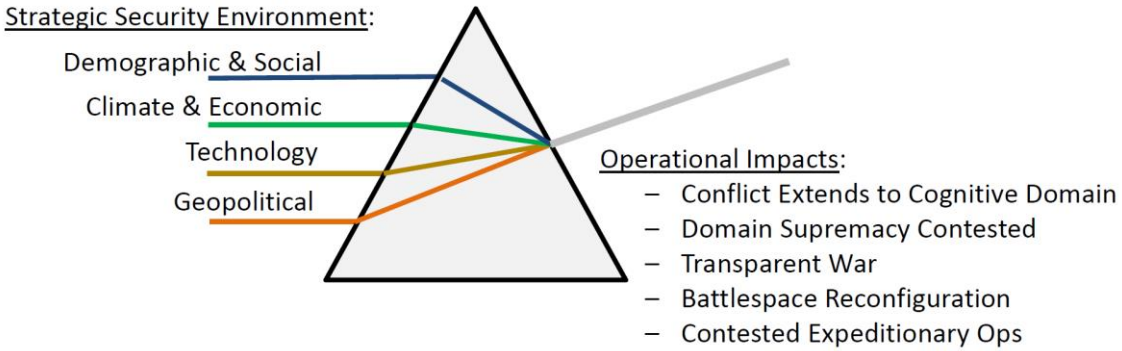


Figure 2.6 Projected Impacts in the Operational Environment

[33] https://chinahistory101.wordpress.com/2017/02/16/infographicchina-mapping-silk-road-initiative-infographicchina-mapping-publications-mercator-institute-for-china-studies/.
[34] NIC, Global Trends.

1. Conflict Extends to Cognitive Dimension – competition of will moves from primarily kinetic to increasingly non-kinetic.

2. Domain Supremacy Contested – the U.S. moves from supremacy in most domains to more lethal and contested in all domains.

3. Transparent War – the U.S. military moves from limited, stove-piped military capabilities in command, control, communications, and computer (C4) and intelligence, surveillance, and reconnaissance (ISR) to continuous and pervasive commercial C4ISR.

4. Battlespace Reconfiguration – from maneuvering primarily in open terrain and contiguous areas of operation to maneuvering in DUAs and dispersed, noncontiguous areas of operation.

5. Contested Expeditionary Operations – from power projection at will to continuously contested power projection across the global commons, from alert to employment.

3. TRENDS AND IMPLICATIONS FOR THE OPERATIONAL ENVIRONMENT

3.1 CONFLICT EXTENDS TO COGNITIVE DIMENSION

As we moved into the 21st Century, the United States' near-peer competitors, China and Russia, have adjusted their approach in employing the instruments of national power (diplomatic, economic, informational, and military) to achieving their political and national security objectives. Military and nonmilitary, particularly informational means, are seamlessly coupled with informational measures receiving increased emphasis (Fig. 3.0). Both countries independently attribute the U.S.'s actions and geopolitical status as the primary motivation for moving toward this concept. The pre-eminent economic and military power, inherent aggressiveness of U.S. capitalism, democratic ideology, and Western media information/influence represent significant threats to their respective regimes' viability and their desire for expansion. Both countries have decided that innovative actions are necessary to improve their regional security and to grow economically. Both have exploited the informational aspect of national power successfully to further their objectives.

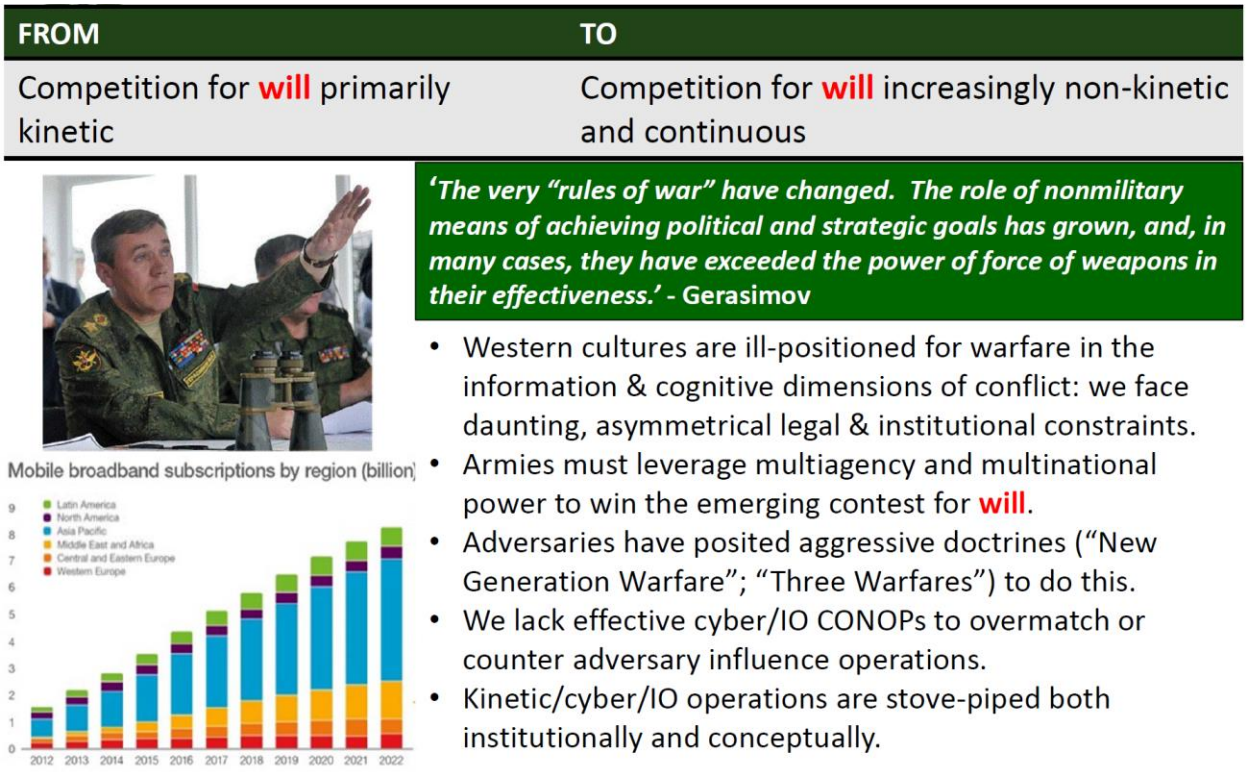


Figure 3.0 Competition in the Cognitive Dimension

3.1.1 CHINA

China announced and began adopting its own concept, "Three Warfares," in 2003, but it wasn't until 2008 that the "Three Warfares" military concept had grown sufficiently to warrant its

inclusion in the OSD annual report to Congress.[35] In the 2011 report to Congress,[36] OSD expanded its description, writing that "Three Warfares," People's Liberation Army (PLA) information warfare concept, are nonmilitary measures aimed at preconditioning key areas of competition to make them more favorable. It was comprised of the following:

- Psychological Warfare – seeks to undermine an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralizing enemy military personnel and supporting civilian populations.

- Media Warfare – aimed at influencing domestic and international public opinion to build support for China's military actions and dissuading an adversary from pursuing actions contrary to China's interests.

- Legal Warfare – used international and domestic law to claim the legal high ground or assert Chinese interests; may be employed to hamstring an adversary's operational freedom, shape the operational space, and build international support to manage possible political repercussions of China's military actions.

The General Political Department is responsible for training all military personnel in the PLA on the full scope of "Three Warfares;" however, the activities of the more tactical organizations (e.g., divisions, regiments, and battalions) seem to be more focused on psychological warfare. Media warfare and legal warfare are more strategic.[37]

The "Three Warfares" concept has melded smoothly into China's historical military traditions and culture. The Chinese regard careful planning and preparation, maneuver, and deception more favorably than sustained violence. In the China's recent writings, there are examples of various successes of the psychological, media, and legal warfare components of the information warfare concept. None dealt with kinetic actions.

The PLA, with its continued military modernization, will be able to achieve resolution of regional conflicts involving land, sea, air, and possibly the offensive and defensive cyber domains. If successful, efforts like these will be "hard" power gains. However, as part of its broader national political objective of increasing what it calls "Comprehensive National Power" (CNP), China would like to create and enhance its "soft" power as well, e.g., with "One Belt, One Road."

Soft power for China entails raising the attractiveness or esteem of the Chinese culture, people, and way of life among other nations and nationalities. Despite censoring the information to its

[35] Office of the Secretary of Defense, Annual Report to Congress – Military Power of the People's of China 2008 (Washington D.C.: Department of Defense, [2008].
[36] Office of the Secretary of Defense (DoD), Military and Security Developments Involving the People's Republic of China 2011, Annual Report to Congress (Washington, DC: DoD, 16 August 2011).
[37] In keeping with Sun Tzu, "For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."

citizens, China's leadership wants to convey to the rest of the world, through the coordinated media, social networks, and information/influence operations, a favorable national identity. It's a competition for dominance in the cognitive dimension of the rest of the world, as nations and nationalities will be persuaded to follow China's lead.

This is a bold vision of the future for China, wrapped in ideals. What if their persuasion is ineffective or refuted? Will persuasion become coercion? Or will it lead to disputes or conflicts? Is China's hidden objective a uni-polar world that it dominates? "Three Warfares," CNP, and "soft" power are aggressive doctrines for regional expansion. Though we haven't seen China transition to combat operations under current geopolitical activity, the Chinese are investing to ensure it remains a viable national security option.

3.1.2 RUSSIA

In 2013, Russia perceived itself as surrounded by enemies. It wasn't a new thought, it's been a belief that has existed since Tsarist times, but with the disintegration of the Soviet Union, the concern had grown more acute. Russia lost the security belt provided by the Warsaw Pact countries, with some former members, (e.g., Poland, Latvia, and Estonia) joining the European Union and NATO. Without the belt of countries, Russia lost the zone where politically dangerous ideas could be stopped before they threatened the Russian leadership's hold on the reins of power. Independent Ukraine, of significant importance to Russia, began looking more to the West, as well.[38]

In February of 2013, Chief of the Russian General Staff, Valery Gerasimov, published, "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations." His article proposed a new Russian way of warfare by combining organized military violence with economic, political, informational, and diplomatic actions to achieve its political objectives. The article was published about a year before the Maidan protests that set in motion the events leading to the eventual annexation of Crimea and the Russian sponsored insurrection in eastern Ukraine.[39]

General Gerasimov named his concept New Generation Warfare (NGW). Although "Warfare" is in the name, he considers it much more than a military conflict. In fact, nonmilitary measures dominate military measures by a factor of 4:1. In "Understanding Russia's Concept for Total War in Europe," Dr. Murphy writes, "NGW is a concept for fighting total war in Europe, across all fronts – political, economic, informational, cyber- simultaneously through fear and intimidation without launching a large-scale attack. If fighting is required, it is highly networked and multi-directional. The stakes can be raised rapidly, possibly without limit."[40]

[38] "Understanding Russia's Concept for Total War in Europe", Martin M. Murphy, PhD, September 12, 2016, The Heritage Foundation.
[39] Getting Gerasimov Right", Charles K. Bartles, Jan-Feb 2016 Military Review.
[40] Op. cit. Murphy.

Clearly, Russia has reverted to its Soviet roots to find some of the means for NGW. Lenin built upon Clausewitz when he made no distinction between the military and civilian roles. He also emphasized propaganda, believing the veracity of the message had little value. What mattered was the effects the message achieved. Terrorism, liberally applied to advance the cause, became a legitimate tool of war. The successful Crimea annexation and asymmetric operations in eastern Ukraine are examples of NGW.

General Gerasimov doesn't view NGW as settled doctrine. Rather, he states, "Each war represents an isolated case, requiring an understanding of its own particular logic, its own unique character."[41] Even so, there are certain similarities in the Ukraine operations. Focusing solely on IO, Russia deployed many government assets to find military, political, or economic weaknesses which could be exploited. The IO campaign began by obtaining media assets such as the RT network, which it could control. Non- Ukrainian governmental organizations were persuaded to support Russian policies. Additionally, diplomatic and media narratives were established to support the actions by those who oppose the Ukrainian government.

Through NGW, Russia has brought war back to Europe in a hidden, undeclared, and ambiguous form. Also, despite Russia's use of military operations and the breaking of treaty agreements, neither the U.S. nor its European allies have responded militarily. Thus, the information war was successful at all levels. The Ukrainian defense was confused and isolated. Russia's denial program in the West was also successful in moving war into the cognitive dimension.

3.2 DOMAIN SUPREMACY IS CONTESTED

The future erosion of U.S. supremacy in every domain is both real and apparent. Increasingly aggressive challengers are developing and fielding a full range of modern, advanced military capabilities. Investments in EW and space systems threaten U.S. command and control, while forward bases, naval vessels, and aircraft are menaced by integrated air defenses and long-range cruise and ballistic missile systems. The ability of the Joint Force to operate effectively in the air and maritime domains hundreds of miles from adversary coasts has eroded, and large land formations are increasingly ranged by accurate fires of increased volume. Rather than exercising supremacy in all domains, U.S. forces will be contested in all domains, encountering more lethal operations, and cannot assume sanctuary in any part of any domain.

The nature of future peer-competitor tactical engagements will reflect the loss of U.S. advantage in each domain. The study team believes future tactical engagements will follow these fundamental characteristics (Fig. 3.1):

- Compressed in Time – the speed of battle at the engagement level will accelerate, collapsing the decision-action cycle to micro-seconds. In many cases, autonomous systems will be needed to deal with the complexity, scale, and speed of engagement decisions.

[41] Op. cit. Bartles.

- Extended in Space – the range of sensors and weapons will progressively extend, expanding the battlefield both physically (with respect to geography and space) and virtually (cyberspace). This will enable competitors to affect each other at extraordinary depth – even globally – as capabilities with far greater range proliferate across all domains.[42]

- Far More Lethal – complex and lethal engagements will permeate the battlespace. Land, sea, air, and space platforms encounter long range precision munitions, highly accurate guided missiles, lasers and microwave weaponry, stealthy and agile swarming robotic systems, and continuous probing of cyber systems. This contest extends to both control and use of the entire electromagnetic spectrum.

- Connected Across Domains (air/land/sea/space/cyber) – lethal engagements are not only characteristic within each domain, but also between them. The range and precision of sensors and weapons allows routine cross-domain engagement. Forces without countermeasures and defenses integrated across all domains are quickly degraded.

- Interactive Across the Conflict Dimensions (physical/informational/cognitive) – engagements will interact not only across every domain in the physical dimension, but also the cognitive dimension, and even the moral dimension of belief and values. Information will be weaponized, either directly through cyber techniques or implicitly through social media techniques.[43] Commanders will recognize the leverage for understanding and appreciating the belief systems that motivate actors in the moral dimension of conflict but confront daunting asymmetric cognitive limitations vis-a-vis our adversaries.[44]

[42] CSA SSG Concept 2.5 p 5.
[43] Army TRADOC G2, *Mad Scientist 2016: The 2050 Cyber Army*, (7 November 2016), p. 36.
[44] Getting Gerasimov Right, Bartles, Military Review.

FROM	TO
Supremacy in all domains	More lethal and contested in all domains

- Tactical engagements are
  - compressed in time
  - extended in space
  - more lethal
  - connected across domains (air/land/sea/space/cyber)
  - interactive across the conflict dimensions (physical/informational/cognitive)

- Tactical engagements in physical dimension favor the defense; information dimension will be continuous and favors the offense. Protracted operations more likely.
- MUM-T required to survive more lethal battlespace.
- Land forces must leverage UAS/RAS to regain local air dominance and enable maneuver.
- Innovative CONOPs required to leverage disruptive technologies into advanced combined arms capabilities.
- Current Army capability development process suboptimal to enable advanced combined arms capabilities development.

Figure 3.1 Characteristics of Tactical Engagements

Tactical engagements in the physical dimension will favor the defense. With peer competitors robustly but equally equipped with sensors and precision weapons, the combatant who moves, particularly over extended strategic and operational distances, is disadvantaged. A defensive stance favors the development of more effective systems of robust, passive sensors and offers the advantage of hardened, redundant locations in the lethality versus survivability contest.

Conversely, offense has the upper hand in the information dimension of conflict. Offensive informational action is generally ascendant and can set the conditions to overcome defensive advantages in the physical realm. The ideal offensive scheme is one beginning with a sustained information campaign that sets the conditions for a surprise, rapid *fait accompli* in the physical realm that can be preserved through follow-on defensive action. Between peer competitors, however, it will be difficult to string together a series of successful offensive engagements. Protracted operations are more likely.

As protection becomes less feasible for land platforms, vehicles will logically follow trends from the air domain and trade passive protection for mobility, speed, and the safety of remote controls. The disaggregation of armored combat vehicle platforms and manned-unmanned teaming (MUM-T) for both sensing and striking systems will enhance initial engagement survivability in a highly lethal battlespace.[45]

[45] ASB Robotic and Autonomous Systems Study, Heinz, 2016.

With major air platforms constrained to remote stand-off distances in a peer-competitor environment, land forces must leverage UAS and RAS to regain the local air dominance necessary to enable ground maneuver, just as they enable maneuver in the aerospace and maritime domains.

Innovative CONOPs will be required to leverage disruptive technologies into advanced combined arms capabilities. The CONOPS must recognize the peer or near-peer status, the proliferation of precision weapons, the expanding reach of sensors and weapons, and the concomitant expansion of the battlefield. They must address the relative advantages and disadvantages of the available technologies and combine them for maximum leverage across all domains. Universal concepts will be problematic, for an operational concept must address the strategic and regional circumstances unique to each adversary, accounting for their specific "way of warfare."

3.3 TRANSPARENT WAR

Today, billions of people worldwide enjoy wireless access to a commercial communications network. Although the network is comprised of complex engineering, its top-level functionality is relatively simple to describe.

To access the commercial network, an individual uses a smart, intuitive, user-friendly wireless device (cell phone, laptop, tablet, etc.) to send a data message or a voice/telephone call to one or more individuals. Typically, the RF transmission from the individual's device travels to a fixed cellular tower or a fixed wireless access point where, in both cases, it's routed and switched via very high capacity cable and RF trunks. As the message or call gets near its destination, it automatically leaves the high capacity trunks and moves to a single wireless or wired connection. At that point, it connects to the target individual's device, enabling voice or message communications. Cellular capable user devices can operate on the move, connecting to one fixed cellular site's high capacity trunks and then getting handed off automatically to another cellular site without noticeable communications interruption.

Commercial wireless devices and the fixed high capacity trunks are constructed and engineered to standards that ensure the network seamlessly connects. Compatible software code recognizes and acts upon the message at each connection. In the commercial network, additional equipment and sites are added frequently to improve the network's coverage and resiliency. Hardware and software technology are continuously upgraded to improve features of the user's device and the speed of the high capacity trunks.

To date, global investment in the commercial network has exceeded trillions of dollars, and it continues to increase with satellite internet constellations like Iridium, OneWeb, and SpaceX Starlink.

FROM	TO
Limited, stove-piped, military C4ISR	Continuous & pervasive commercial C4ISR

- Network:
  - 50 billion devices connected to global Fiber/RF/SATCOM nodes
  - Dense EM and Cyber environments, commercial communications
- Sensor:
  - Explosive growth of **commercial** ISR from satellites, drones and IOT
  - Sophisticated ISR available to DoD, near-peer & violent non-state actors alike
- Operational transparency increasing and beyond state control.
- Relentless and continuous fight for connectivity via IO, cyber and EW.
- C2 capabilities augmented at lower echelons.
- Sensor, processing, and engagement speeds shift decision space increasingly to machines via AI.
- Increased combat support effects from CONUS to dispersed forward forces.

Figure 3.2 Transparent Warfare

There will also be explosive growth in commercial ISR from satellites, drones, and the Internet of Things (IoT). Information will be readily available to DoD, near-peers, and non-state actors alike. Sensor processing and engagement speeds shift the decision space increasingly to machines and AI. Below threshold hostile activities and criminal activities will continue to attempt to usurp good order by disrupting connectivity via cyber, IO, and EW.

The use of small satellites (e.g. Cubesats) for imagery and other forms of sensing is rapidly making low cost intelligence networks available to anyone with a credit card. One Finnish company, IceEye, has 30 synthetic imaging radar (SAR) satellites that can image the earth even under clouds. [46] These inexpensive sensor networks are commercial competitors to exquisite systems built and managed by the U.S. and its peer competitors. Another area of information growth involves the use of unmanned aerial and undersea autonomous systems and the data they produce about the world. The ready access to the world's open source information will be available to all except those who are restricted by their governments.

The U.S. military is also competing with advances in commercial communication because its air-land tactical network operates similarly to commercial Wi-Fi and cellular networks, with a few significant differences. The operational conditions are more demanding, and traffic needs to be protected with government approved encryption. Both the user devices and the various RF links, to include high capacity trunks, must operate on the move in rugged terrain. They're also required to operate in the full range of worldwide temperature, humidity, and environmental

[46] https://www.iceye.com/.

conditions (e.g., sand, dust, rain, saltwater, etc.), and they need to provide reliable communications in built-up cities, dense wooded areas, and mountainous terrain.

The military communications network must survive operating in an increasingly sophisticated hostile electromagnetic and cyber environment. The RF devices are subject to monitoring, jamming, spoofing, and damaging cyberattacks. Lacking protection and mitigating measures, military RF emissions can be identified, located, and targeted by the enemy.

The Army has used multiple PORs over the past three decades to design, acquire, and field specialized terminals, RF links, and networks comprised of various individual wireless devices, single channel radios, and high capacity, multi-channel/trunk radios. Each of these PORs was built and tested and complied with the contract specifications deemed necessary for successful operation. Unfortunately, the specialized RF links and networks were not required to operate seamlessly with one another.

That one shortfall exists for a significant number, if not the majority, of the Army's PORs, which has created a suite of stove-piped networks with limited interoperability. As a result, the C4ISR System in the Army today and programmed to be fielded in the next decade isn't sufficiently effective to meet the Army's operational needs. The Institute for Defense Analysis (IDA) cited in a detailed report released in May 2017 that the Army's PORs, "Fall short of demonstrating a survivable, effective and suitable air-land tactical network that meets the need of the warfighter."[47] From a survivability standpoint, very few of the waveforms have anti-jam capabilities incorporated. Additionally, waveforms operate in self-organizing, Mobile Ad Hoc Networks. In such a network, the radios must transmit frequently to update the status of each member of the network, which in turn increases their electromagnetic signature and vulnerability to enemy targeting.Beyond the ten-year time frame, the commercial communications system will have dramatically changed, characterized by Increased speed and connectivity, coupled with hardware needing less size, weight and power. The military will migrate a majority of its tactical communications network to commercial sources. User devices will become more intuitive, smaller, and possibly embedded into the individual. Extremely high frequency (30-300 GHz) will be used extensively.

3.4 BATTLESPACE RECONFIGURATION

For decades, the Army expected to fight in battlespace that would be generally open, rural geography across contiguous areas of operation. Several factors have contributed to changing that condition. Future maneuver will routinely occur in dense urban areas (DUA) and/or dispersed and noncontiguous operational areas (Fig. 3.3).

[47] A Comprehensive Assessment of the Army's Air-Land Mobile Tactical Communications Network", Marwick, M.S. Project Leader, Laprade, E.J., 2017, IDA, Alexandria, VA.

FROM	TO
Maneuver primarily in open terrain & contiguous areas of operation	Maneuver extends to Dense Urban Areas & dispersed, noncontiguous areas of operation

- Conflict in Dense Urban Operations increases, as urban areas expand and all competitors seek:
  - Concealment from ubiquitous sensors
  - Overhead cover from peer-capable engagement systems
- Cities become a necessity – even an opportunity -- for foraging, e.g., water, energy, 3D printing materials, communications, transportation assets
- "Pulse logistics" v. "Continuous logistics"
- U.S. CONOPs that "destroy to save" are no longer acceptable; non-combatants planning may shape and define the outcome
- IPB/SA to include culture, history and patterns of life
- Units will disperse and disaggregate to frustrate detection and engagement; wide area control less feasible and battlespace non-contiguous
- Combined and Joint capabilities migrate to lower echelons
- Units must mass effects vice forces: range overmatch at a premium for both sensors and weapons
- Dispersed forces constantly on the move need beyond line of sight connectivity
- Comms across a non-contiguous battlespace far from assured; advanced Mission Command must enable subordinate recognition/action when mission should change

Figure 3.3 Battlespace Reconfiguration

DUAs have historically challenged land U.S. forces (e.g., Manila, Sadr City, Mosul) but by mid-century, they'll be far more pervasive and populated due to changing demographics and world economic growth. Urban environments will sprawl horizontally and vertically in space, but also socially, posing both challenges and opportunities. Land forces must operate in these areas for sustained periods and will view such operations as the norm, vice the exception. Urban areas will be particularly attractive because peer competitors will seek the complex clutter of large built-up areas for both concealment from ubiquitous sensors, as well as the abundant available overhead cover that offers some protection from peer-capable weapons systems.

As it becomes necessary to conduct urban operations, opportunities will also emerge. Cities will become "smarter" and more instrumented by a vast array of cheap and connected sensors measuring traffic, human, and material flows. They'll also have massive resources that can be directed for war, such as computer-controlled machine shops, 3D manufacturing facilities, small-scale chip foundries, and a dense selection of consumer electronics, wireless nodes, and commercial and private fiber networks. There will be ample opportunities for foraging for water, energy, 3D printing materials, and communication and transportation assets.

Urban verticality and subterranean infrastructure will complicate land force operations, freedom of movement, and force protection requirements. Some combatants will continue to employ the "control by devastation," technique of previous wars, while others will seek very precise, low collateral damage combat. There will be a premium on the ability to separate combatants from non-combatants in dense urban environments. Forces will employ sophisticated human and cultural mapping, biometric assessment, and tagging at long range,

and other technologies that enable combat forces to understand and to selectively control city services and utilities. U.S. CONOPs that "destroy to save" will become obsolete, as controlling the critical infrastructure, economic zones, flows of people will be necessary to winning in DUAs.

Non-combatant considerations—including preserving both life and quality of life—may become the dominant factors that shape and define the outcome of military operations. Key planning functions such as intelligence, preparation of the battlefield, and situational awareness will need to focus on and emphasize cultural factors, historical considerations, and predominant patterns of life.

Outside of large urban areas, units will disperse and disaggregate to frustrate detection by ubiquitous sensor networks and associated weapons systems. U.S. Army units will need to mass effects, not forces. Consequently, range overmatch will be at a premium for both sensors and weapons. The requirement to disperse, disaggregate, and conceal will make wide area control less feasible. Any battlespace reliably "controlled" in a traditional sense by military forces will be typically non-contiguous. In this new rendition of a battlespace, with ubiquitous sensors and long-range, precision engagement systems, the likelihood of surprise, engagement, and destruction won't be significantly different between areas previously described as "deep," "close," and "rear."

In that new battlespace, sustainment will no longer be a continuous background function over linear lines of communication. Rather, logistics will require an overt, integrated, combined arms activity that "pulses" and protects support packages across non-contiguous battlespaces. A successful sustainment pulse resets a unit's "expiration clock," but that clock inexorably counts down until the next sustainment pulse is delivered.

Communications across a non-contiguous battlespace will be uncertain, with persistent and pervasive attacks on networks in all domains, from space to local radios, through cyber, integrated EW, and other means. Adversaries will contest communication wherever possible,

organization-to-organization, man-to-man, man-to-machine, machine-to-machine, etc. That contest will prove crucial for dispersed and disaggregated forces. Competitors will seek assured communication through redundant, heterogeneous networks, employing innovative techniques, including low power and highly directional transmissions over multiple portions of the electromagnetic spectrum. Dispersed forces constantly on the move will need continuous beyond-line-of-sight connectivity, such as through SATCOM and digital HF.

The sustainment challenges will be significant. Life will almost certainly be extremely austere. Water, chow, ammo, fuel, maintenance, and medical support will be about all we should plan for… and our lines of communication will for sure be contested, and probably denied. Being surrounded will become the norm, the routine, the life of a unit in combat. In short, learning to be comfortable with being seriously miserable every single minute of every day will have to become a way of life for an Army on the battlefield that I see coming.

GEN Mark Milley, CSA, 2016

Anticipating extensive periods of interrupted communication, the study team predicts combined arms and Joint capabilities will migrate to lower echelons, creating a demand for flexible, scalable force structures that can accommodate joint and combined capabilities, disaggregated to lower levels or aggregated without loss of efficiency. Super-enabled, small unit formations will reinforce the need for innovative approaches to generating joint and combined arms synergy.

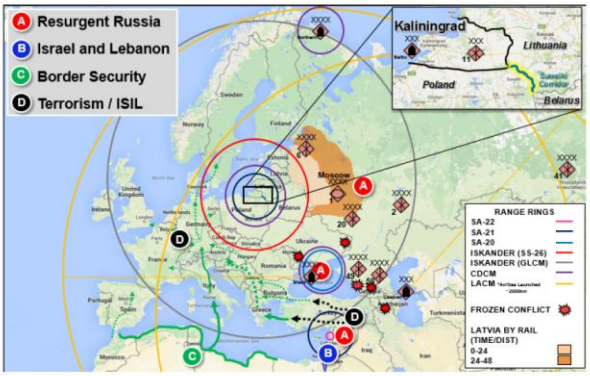
In such a reconfigured battlespace, mission command will evolve substantively. A commander's original intent will rarely persist for extended periods, so the rapid presentation of tactical threats and opportunities will require an advanced level of mission command. Subordinate commanders must be willing to initiate significant new missions based on recognition of new, emerging conditions, without the traditional, positive confirmation or refinement of original missions. Seasoned, experienced, and well-trained leaders will need to be grown to operate in these uncertain tactical environments.

3.5 CONTESTED EXPEDITIONARY OPERATIONS

U.S. Army units are under constant surveillance (ISR) by adversaries taking advantage of ubiquitous sensors, from commercial imagery to the IoT, operating over global civilian and military networks. Strategic surprise will be challenged by near-peer adversaries able to constantly monitor U.S. deployments from home station to the operational area (Fig. 3.4).

FROM	TO
Power projection "at will"	Continuously contested from alert to employment

- Constant surveillance - Ubiquitous sensors & networks in use from home station to employment - adversary constantly aware
- Deploying forces continuously at risk of **lethal engagement** in multiple domains
- Robust A2/AD regimes restricts expeditionary maneuver into expected areas of entry
- Peer competitors may conduct expeditionary operations as well (e.g., Djibouti)
- Requires mass from fires and maneuver of dispersed, covert, concentrated, small unit forces to achieve surprise
- Retain and leverage forward presence
- Land forces must fight into and under an enemy A2/AD regime



Illustrative A2/AD environment

Figure 3.4 Expeditionary Operations

Deploying forces will be at risk of engagement in multiple domains starting with early stage cyber and information warfare attacks aimed at delaying early entry. Robust A2/AD defenses will restrict expeditionary maneuver into expected areas of entry. With the advancement in long range precision fires, A2/AD would endanger U.S. land and air forces at the edge of the theater of combat.

It's unlikely peer competitors will cede expeditionary warfare to the U.S., as they've demonstrated their own expeditionary capabilities (Russia in Syria and the Chinese in Djibouti). This increases the potential for an immediate clash in traditionally remote regions where the U.S. has traditionally moved and operated unchallenged.

Success in such an environment will require an "en masse impact" from fires and the maneuver of dispersed, covert, concentrated small units to achieve local surprise. More importantly, the U.S. will need to retain and leverage forward presence in Central Europe and Asia to leverage the advantages of the tactical defense, minimize the nominally long delay of moving expeditionary forces into theater, and to reduce exposure to long range fires. Even then, land forces will need to fight into and under a robust enemy A2/AD regime.

4.0 CAPABILITY CONTRAINTS

The complexity and uncertainty of the future SSE present a plethora of operational challenges to the Army. One of the SSE trends having particularly important implications is the commercialization and diffusion of technologies around RAS, AI, and human enhancement, areas expected to experience exponential growth over the next decades. These technologies will become available to friend and foe alike. In such an environment of technological parity, the Army will be challenged to maintain (or recover) overmatch against adversaries with like capabilities. Overmatch will depend on the superiority of U.S. integration of the technologies into DOTMLPF capabilities and of the CONOPs and TTPs for employing those solutions.

An equally important challenge will be the abundance of potentially disruptive technology investment options available to the Army in the short-term to modernize the future Army in the 2030-2050 timeframe. Judicious decisions must be made in the context of constraints that affect the Army's ability to fund development and procurement of future capabilities, to rapidly field the capabilities, and to adapt future capabilities in an uncertain environment in which adversaries enjoy legal and ethical asymmetries. These constraints require that the Army employ a CDS that ensures not only making the right choices on big bets (i.e., technologies that yield high payoff with some risk), but also providing maximum flexibility and adaptability in fielding and employing them.

4.1 FISCAL CONSTRAINTS

The first constraint facing the Army over the next decade is a potentially a tough fiscal environment. In the absence of a major conflict, the Army's Total Obligation Authority (TOA) may fluctuate under different administrations but may not grow substantially over the long term. A possible scenario will be a decreasing TOA, driven by the squeeze on discretionary funding accounts (including Defense) within the federal budget caused by growing non-discretionary accounts (e.g., Social Security, Medicare, and Medicaid), as well as interest on the growing national debt. The Government Accounting Office[48] projects that the national debt will exceed 100% of Gross National Product (GNP) around 2030, further pressuring the solvency of social welfare accounts (Fig. 4.0).

[48] GAO-17- 237SP, Action is Needed to Address the Federal Government's Fiscal Future, 17 Jan 17

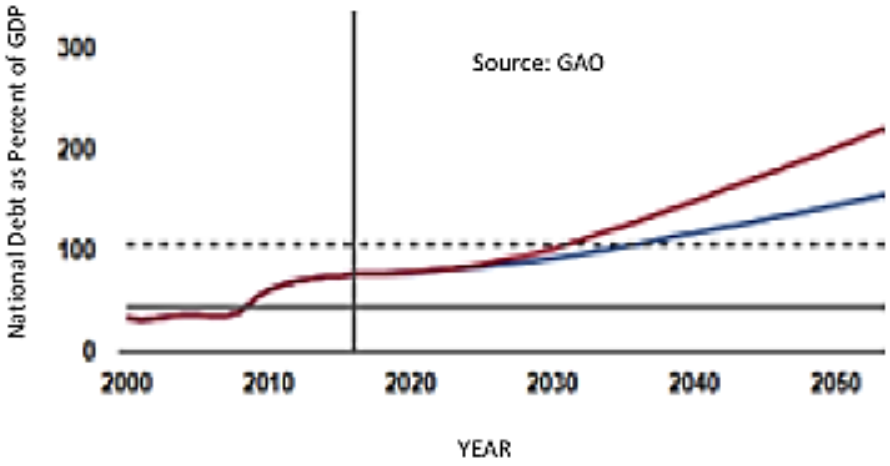


Figure 4.0 National Debt as a Percent of GDP

Within this fiscal environment, Army modernization budgets are particularly vulnerable because readiness will continue to be the funding priority as current optempo is not projected to drop in the near future. The Army can't expect to offset its stagnant or declining R&D by capitalizing on other federal R&D spending, which have experienced similar pressures (Fig. 4.1). Thus, while enjoying an abundance of modernization investment opportunities due to the exponential technology growth, the Army will be confronted with making difficult choices on which of the opportunities to place its big bets. Adding to this dilemma, choices will have to be made in the face of uncertainties about how the SSE trends will play out in affecting the OE.

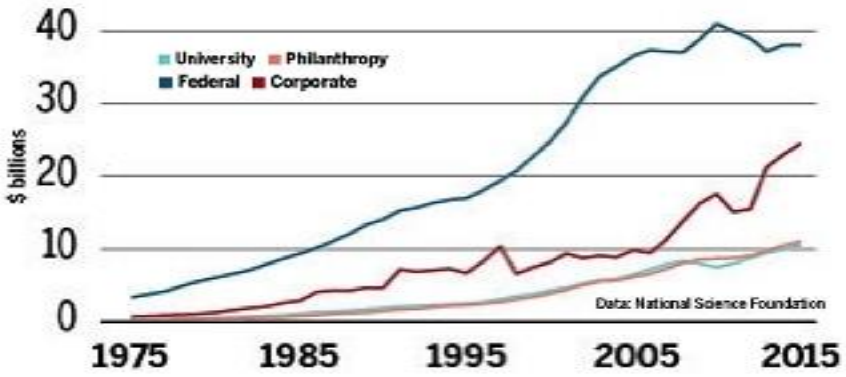


Figure 4.1 R&D Expenditures

The Army will need to look more to the private sector as the source of innovation in making technology-driven modernization investment decisions. While commercial R&D is expected to grow, the investment growth will not uniformly apply to all market segments. For example, the global markets for manned rotorcraft systems has leveled off in recent years and is expected to experience a decline, as the demand decreases for manned civil and commercial rotorcraft needed to service the oil industry. As a result, investment and innovation in this market segment will become increasingly dependent on the military, and the Army will find relying on

private sector R&D as a primary or supplemental source of advanced manned aircraft technology increasingly difficult (Fig. 4.2).

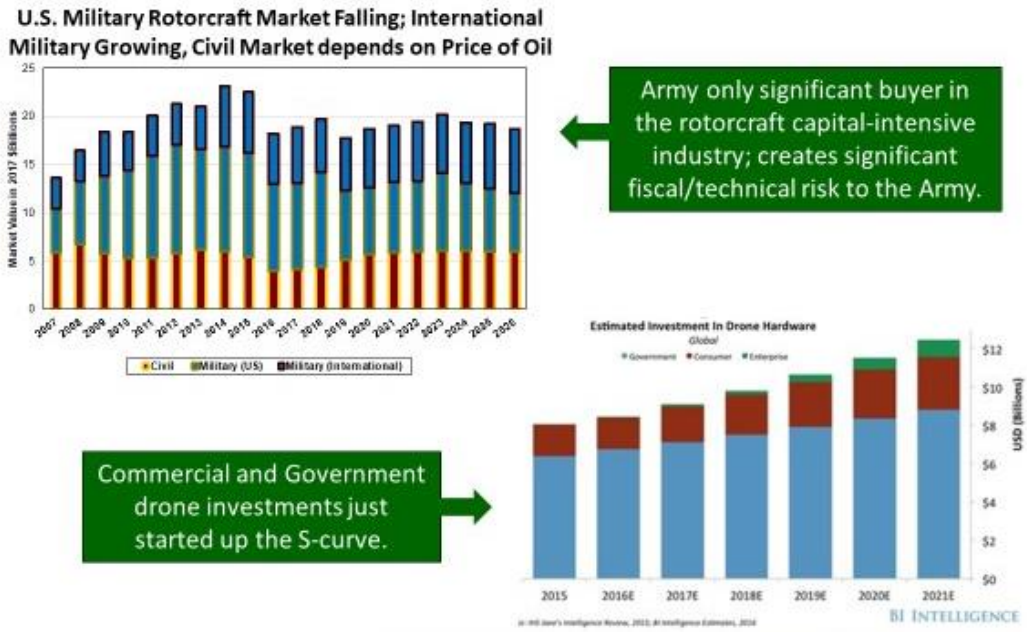


Figure 4.2 Projected Rotorcraft Markets

In contrast, commercial investments in UAS and UAVs are increasing and driving the civil and commercial markets (e.g., precision agriculture, infrastructure inspection, electric grid monitoring) up the S-curve. Given the Army's limited R&D budget, the Army will need to carefully weigh investment in future manned versus unmanned systems that can perform the same functions. This is an illustrative example of the type of tradeoffs the Army will need to apply to other technologies and applications as well.[49]

4.2 ACQUISITION CONSTRAINTS

The second constraint the Army faces in fielding disruptive capabilities comes from the asymmetry in acquisition timelines between the DoD's formal acquisition process and adversaries' more nimble procurement processes. There have been multiple attempts over the past several decades to reform and streamline DoD acquisition and fielding of new PORs, including the Joint Capabilities Integration Development System (JCIDS) requirements development process; the DoD 5000 rules and regulations for POR development and procurement; the Planning, Programming, Budget, and Execution (PPBE) process; and Operational Test and Evaluation (OT&E); but attempts at reform have made the overall life cycle management system even more complex (Fig. 4.2).

[49] Teal Group research http://www.businessinsider.com/the-drones-report-market-forecasts-key-players-and-use-cases-and-regulatory-barriers-to-the-proliferation-of-drones-2016-3.

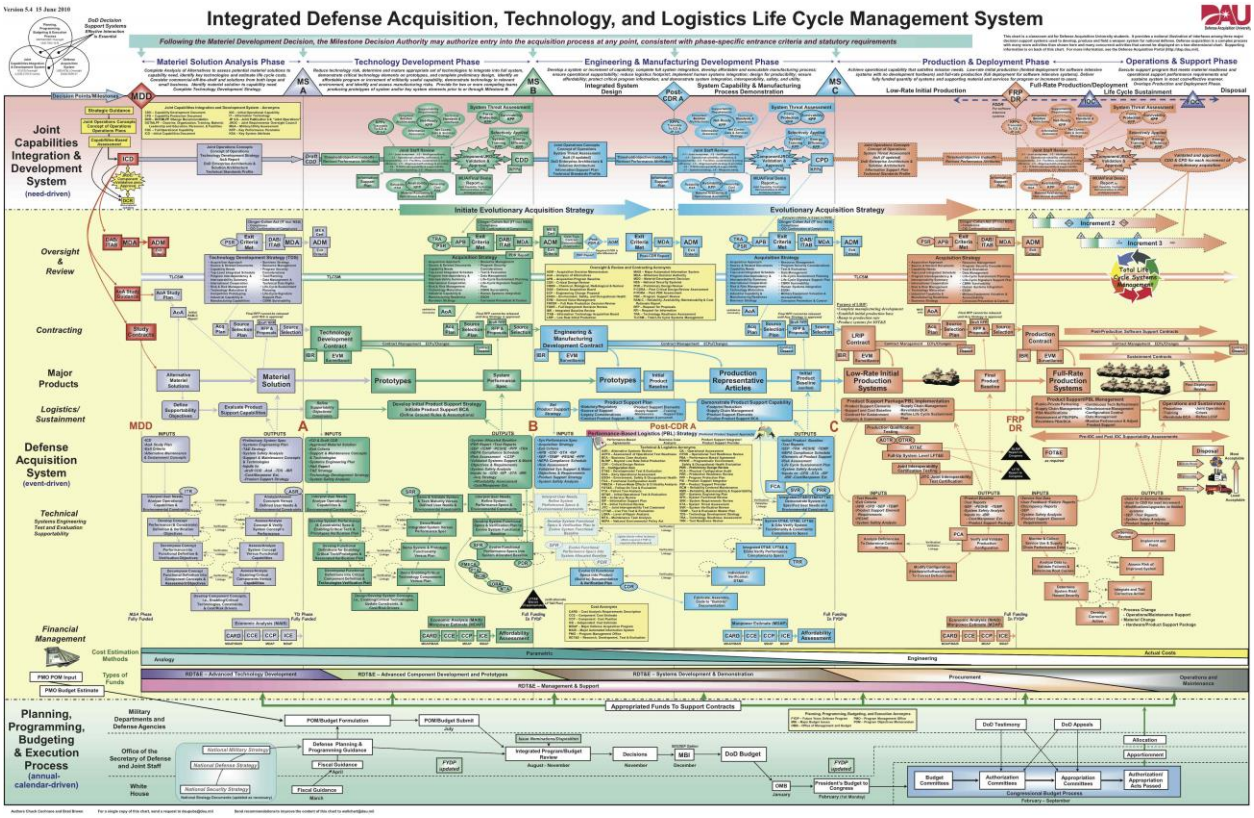


Figure 4.3 Integrated Defense Acquisition System[50]

Despite the reform efforts, it's not unusual for the time from definition of a new system Initial Capability Document to Initial Operating Capability (IOC) to be in the range of 10 to 15 years. While 2030 is the distant future in terms of SSE uncertainties and S-curve cycles for commercial capabilities (considering, for example, the I-phone was introduced only 10 years ago), it's only one acquisition cycle away for any new POR to reach IOC status. Moreover, procurement of systems with FOC may take another 15 to 20 years due to procurement budget constraints. Under the current system, procurement buyout of the POR system can easily stretch out to the far end of the 2030 to2050 timeline.

In contrast, adversaries aren't constrained by such onerous processes. The timelines for development of highly sophisticated systems (e.g., combat aircraft, combat ground vehicles, air defense systems) by peer and near-peer competitors may be protracted because of technological challenges, but not because of self-imposed process restrictions. Additionally, once these systems are developed, they become readily available to other adversaries through unfettered foreign military sales. The full spectrum of U.S. adversaries, from peer to VNSAs, are

[50] DAU Integrated Defense Acquisition, Technology and Logistics Life Cycle Management System, https://dap.dau.mil

proficient at adapting commercial systems or NDIs into instruments of warfare, and rapidly employing them (e.g., ISIS' use of quadcopter drones with lethal capabilities[51]).

The Army and the other military services do have means of rapid fielding outside of the formal acquisition processes. These vehicles are responsive to Joint Urgent Operational Needs (JUONs), usually through the tailoring of NDI and/or commercial systems. Rapid procurements are generally funded outside of the PPBE process by means of the Overseas Contingency Operations (OCO) funding associated with named operations, such as Operation Iraqi Freedom (OIF), and Operation Enduring Freedom (OEF). As these operations wind down, OCO funding is expected to decrease. It's also the case that rapidly acquired capabilities are deployed without full DOTMLPF integration, and don't have a sustainment pipeline. Thus, after the urgent need ceases to exist, the funding for these systems isn't sustained within the POM, and they don't transition to POR status for fully integrated DOTMLPF capabilities. The DoD and the Army continue to search for means of institutionalizing more rapid fielding of tailored NDI capabilities within the formal JCIDS, acquisition, and PPBE processes, but they've had limited success to date.

4.3 ASYMMETRIC LEGAL/ETHICAL CONSTRAINTS

Asymmetries in legal, ethical, and moral norms exist between the U.S. and potential adversaries, particularly VNSAs, which have no compunction over the unfettered use of lethal autonomy and human enhancement, or in causing civilian casualties. They also have no compunction in violating international and multinational treaties that restrict the proliferation of WMD and the use of certain munitions, such as cluster munitions. The U.S. and many of its close allies are perhaps uniquely constrained in the use of similar capabilities by norms associated with democratic societies that respect international law (e.g. spectrum allocation, international boundaries, rights of navigation) and inviolable human rights.

One capability currently being debated at policy levels within the government is the use of AI for lethal applications of RAS. There's much concern within the policy community (sensationalized in the popular press and in motion pictures and video games) about "killer robots." A very clear DoD policy (DODD 3000.0, 2012) requires "appropriate levels of human judgment over the use of force." This guidance is widely interpreted as the need for human "eyes-on-target" for supervisory control over RAS for any lethal action. Adversaries, on the other hand, may not impose the same constraints for lethal RAS on the battlefield, creating an overmatch disadvantage based strictly on policy and ROE. Similar adversary overmatch may result from differing policy, legal, ethical, and treaty-compliance constraints imposed on the use of other disruptive technologies, such as human enhancement and cluster munitions).

[51] Schmitt, E., Papers Offer a Peek at ISIS' Drones, Lethal and Largely Off-the-Shelf, NY Times, Jan. 31, 2017, Retrieved from: https://www.nytimes.com/2017/01/31/world/middleeast/isis-drone-documents.html.

5.0 CAPABILITY DEVELOPMENT STRATEGY

With the myriad of challenges, the future SSE and OE also present numerous opportunities for the Army. Many potentially disruptive capabilities are on the cusp of exponential growth. The Army will need to make well-informed, trade-off decisions on which few specific capabilities it should select out of the many available to place its big bets regarding modernization for 2030 and beyond. A CDS that facilitates the selection, development, rapid fielding, and innovative employment of those big bets (within the identified constraints) is essential to retaining overmatch.

The study team developed one potential CDS addressing each of the capability constraints. The objectives of the CDS are to:

1. Gain insights into the operational utility of a proposed capability and to explore innovative CONOPS/TTPs that best exploit the prototype capability to provide a well-informed basis for acquisition decisions on the big bets.

2. Accelerate the Fielding of IOC that prove operational value prior to formal but agile acquisition of FOC.

3. For new capabilities where we currently "self-deter," such as AI-enabled decision aids or human performance enhacements, build in the ability to dynamically activate dormant "war reserve" functionality that respond to battlefield conditions and changes in ROE.

5.1 INTEGRATED OPERATIONAL EXPERIMENTATION AND SIMULATION

The Army has many big bet opportunities emerging from expanding technologies, but fiscal constraints require that it make judicious decisions on the few it can afford. Technological parity also requires the Army do a better job than adversaries of integrating technology-enabled capabilities into its force structure, employing them with innovative CONOPS and better utilizing the human element in producing those capabilities.

A key element of a CDS requires use of operational experimentation and simulation to understand how best to (a) employ candidate capability development options, (b) explore effectiveness of organizational and human integration options, and (c) develop innovative CONOPs and TTPs. Experimentation and simulation provide a sound basis of comparison between capabilities competing for limited funding and a solid understanding of the operational requirements and estimated costs for development of the capability.

Operational experimentation is distinct from product-level experiments conducted to improve the technology maturity of a physical system or component. Operational experiments are used to exercise functional interfaces and interactions, and to understand functional performance of a proposed capability within a realistic system-of-systems environment. They can be conducted with physical surrogates that faithfully represent the functions of the proposed capability and

that stimulate functional interactions with other systems (e.g., command, control, and communications). Such experiments would be like the Army's Advanced Warfighting Experiments but more focused on a single capability (rather than many) to clearly delineate the change in operational utility and effectiveness of the single capability. The change in utility would be measured by the difference in measures of effectiveness between a control team not having the proposed capability and a capability-enhanced team. Both teams would operate against a red-force team and would have opportunities for learning through multiple iterations of the exercise.

Operational experiments would typically operate in a combined live, virtual, and constructive simulation environment. High fidelity simulation is an important component in several ways. First, it reduces the cost and burden of conducting the experiment by emulating many of the interfacing systems. Second, because the experiments can be conducted with only a limited set of scenarios, threat capabilities, and operational conditions, the simulation, once validated through the experimental results, can be used to extrapolate the results to a much wider set of scenarios, threats, and conditions. Also, much of the software functionality for the proposed capability can be embedded in the simulation. This is particularly useful for AI-enabled capabilities in which the non-deterministic behavior of the system (e.g., RAS) is difficult to predict. The behavior and transparency of the system can be calibrated under differing conditions to optimize human-machine interactions and to improve trust.

Many, or most, new capability solutions will cut across Army Centers of Excellence (COEs). The CDS must account for the need for multi-COE participation in the experiments to ensure cross fertilization among COEs in the design and conduct of the experiments, development, and validation of the simulations. A good example of the need for participation across COEs is the expanded use of UAS to meet the needs of multiple COEs. The Aviation COE is responsible for design and development of UAS, but advocacy for specific UAS missions cuts across several COEs (e.g., Fires COE for targeting or for conducting SEAD, Log COE for supply delivery, Intelligence COE for ISR, etc.). The tendency would be for each COE to require a unique UAS platform and sensors for its mission; however, as indicated in the 2016 ASB study on Robotic and Autonomous Systems, it's feasible to develop modular payload UAS's that can provide capabilities across multiple missions. Such cost-effective solutions require coordination that can bridge the daunting barriers between many of the current "stovepipes of excellence."[52]

5.2 PROTOTYPING FOR EARLY FIELDING OF LIMITED OPERATIONAL CAPABILITY

The Army's inability to field new, major system PORs under the DoD formal JCIDS, DoD 5000 acquisition, PPBE, and OT&E processes provide adversaries, unencumbered by formal acquisition processes, with an asymmetric advantage in the ability to rapidly field new capabilities.

[52] Op. cit. Robotic and Autonomous Systems of Systems Architecture

An approach that would facilitate earlier fielding of capabilities that could be institutionalized within the formal acquisition processes, without using JUONS and OCO funding, involves advanced prototyping. The study team identified a promising model in the Joint Capability Technology Demonstration (JCTD) type of purpose-built prototype, used when the prototyped system has limited operational capability and the project has residual assets that could be deployed into a theatre.

The principal differences between the proposed, JCTD-type of prototyping and the standard Technology Maturation and Risk Reduction (TMRR) type of prototyping (part of a POR) are that (a) the project would have the objective from the outset of providing deployable assets, and (b) it wouldn't necessarily be funded through a POR. While JCTD-like, the project wouldn't have to be Joint, i.e., funded through OSD. Instead, it would be funded and directed through Army 6.3/6.4 budget authority and contracted by means of agile contracting methods, such as Other Transaction Agreements (OTA). The prototype needs to be of sufficient design and performance fidelity that it offers a path from LOC to FOC without significant redesign of the prototype, contingent upon a successful proof of operational value during the prototyping project and subsequent in-theatre operations. This proposed approach would have the added advantage of transitioning the prototype to a POR by proceeding directly to a Milestone B acquisition decision.

These prototyping projects differ from the operational experiments described above in that the prototype projects develop physical systems, while the experiments evaluate functional attributes by emulating the physical systems using surrogates. While the experimentation and prototyping may be conducted separately, synergies can also be attained by coupling the projects for a candidate disruptive capability.

The proposed JCTD-like prototyping efforts are promising for use with major platform systems, such as manned or unmanned ground combat vehicles, UAS and UAV, and Manned-Unmanned Teaming (MUM-T) platforms. For Soldier or network systems, the study team believes the Army should seek alternate approaches for rapid fielding, based on service contracts. Because of the anticipated proliferation of commercial communications and ISR space systems, the Army network will likely increasingly use and exploit commercial systems. It may be advantageous for the Army to field improved C4ISR capabilities by some means other than the tedious FAR acquisition processes, such as nimbler service contracts with the commercial operators.

5.3 DYNAMIC ADAPTABILITY TO CHANGING ROE

Many of the technologies that will contribute to the CFW have legal and ethical issues associated with their employment, including: AI for lethal RAS; human enhancement; weapons or munitions with indiscriminate, highly lethal effects; and the intentional distortion of information through social media. U.S. adversaries enjoy potentially devastating overmatch advantages with their lack of legal and ethical constraints on the development and use of these technologies.

U.S. policies will continue to be shaped by the acceptable norms of our free society and not subject to the degrading norms of some adversaries. However, in past conflicts, the U.S. has changed policies and ROEs to accord with battlefield realities. To be prepared for these kinds of adjustments in future conflicts, the Army may need to conduct R&D to mature technologies that enable emplacing latent capabilities to be utilized if circumstances require.

The Army may proceed in this vein with lethal RAS. Adversaries are already employing lethal capabilities delivered indiscriminately from commercial UAS. Peer and near-peer adversaries are developing highly lethal, autonomous ground robotic vehicles and air vehicles. The Army's quite capable of developing similar systems but is constrained in transitioning such capabilities from R&D to PORs by DoD policy. The study team believes a concept of "dynamic autonomy" provides a path for breaking through the transition roadblock while still complying with current policy and ROE restrictions.[53]

With dynamic autonomy, capabilities for greater autonomy can be designed from the outset into any new RAS yet remain dormant until dynamically activated on the battlefield as ROEs change. For example, a ground robotic tank can be operated initially under remote control from manned supervisory vehicles to ensure human "eyes-on-target" before the RAS fires its rounds. Autonomous functionality embedded in the RAS control system can be triggered to allow various incremental autonomous functions, from automatic slewing of the gun turret to source of fire and all the way to autonomous lethal engagement.

Rapidly improving AI capabilities anticipated over the next decade or two require a modular open system architecture (MOSA). The development of any new RAS system can be initiated with limited, mature autonomous functionality that can be continuously improved over time as AI-enabled functionality evolves. An "autonomy roadmap" with MOSA standards would prove to be a powerful design tool for Army RAS to fully and rapidly exploit AI in future conflicts, offsetting asymmetries with the lack of adversary constraints.

[53] Ibid. (For more detailed discussion of dynamic autonomy and autonomy roadmaps for new RAS PORs.)

6.0 FINDINGS AND RECOMMENDATIONS

The study team's survey of future estimates identified a clear consensus of increasing complexity in the SSE. A daunting array of peer and near-peer competitors demonstrates an increasing ability to exploit legacy and emerging technologies, and many of these technologies are accessible to non-state competitors. Consequently, the Army will encounter increasingly diverse and demanding operational challenges. On the positive side of these trends, the Army will find the space of big bet opportunities for the Army expanding. Judicious exploitation of the big bets will enable the Army to restore battlefield overmatch.

Unfortunately, the Army's ability to exploit the range of big bet opportunities is at risk. The Army faces fiscal constraints and policy restrictions that take some big bets off the table for development. In addition, normal acquisition timelines will limit the Army's responsiveness when future battlefield engagements convince the nation to relax or completely forego current policy restrictions.

Therefore, the study team's recommendations include specific areas for Army investment, as well as divestment, to enable big bets. The Army will need agile development strategies to identify the best big bets and innovative CONOPs to best utilize the capabilities derived from them. An agile capability development strategy will dynamically adjust to technology surprises, including policy reversals.

6.1 BIG BETS FOR ENHANCED BATTLE OUTCOMES

Findings:

- Changes to the Character of Future Warfare are inexorable and accelerating, which make maintaining overmatch, without appropriate response, far more difficult. Our adversaries are reducing, if not eliminating, our overmatch.

- Even with Allies' recognition of an existential threat, the U.S. will have to make the preponderance of the Allied national security investment.

- Army leadership has recognized the impact of the Ukrainian war yet has not communicated the solutions for our Army to respond to this type of threat.

- The Army has underinvested in new, fielded munitions since the mid-1980s.

- Easy global access to emerging technologies (Robotic Autonomous Systems (RAS), Cyber, Influence Operations (IO), AI, and human enhancements) are leveling the playing field and increasing lethality.

- The Army has no plan to defeat enemy integrated air defense. Non-developmental Unmanned Aircraft System (UAS), coupled with innovative CONOPs, appears to be a viable approach to mitigate the Integrated Air Defense (IAD) challenge.

- The introduction of ground and air robotic combat vehicles changes both the lethality and survivability parameters.

Recommendations:

- Prioritize MUM-T investments across successive POMs. Focus on ground MUM-T; it is a unique Army capability and will not occur without Army investment. Leverage the efforts of other services for air MUM-T. Exploit commercial AI developments and adapt them for Army-unique applications.

- Increase lethality through new payloads and longer-range fires, area effect munitions, and kinetic energy missiles.

- Invest in:
  - MUM-T armed ground robotic vehicles
  - Commercial network capability for Army participation in Multi-Domain Battle (MDB)
  - Lethality
  - Education, training, cadre, facilities, and infrastructure to enhance overmatch in Soldier (enlisted, warrant officer, and officer) and team performance
  - Cyber, Influence Operations, and EW as Army tactical weapon systems
  - Leverage DARPA innovation (e.g., Cognitive EW, Swarming UAVs & Offset, Squad-X)

- Divest from:
  - Army-developed unique networks that do not meet the needs of MDB
  - Enhancements to armored combat vehicles that add weight
  - Manned aviation platforms and their enhancements not required in a MUM-T environment

6.2 Overcoming Capability Development Constraints

Findings:

- The Army lacks a capability development strategy across Centers of Excellence to exploit:
  - Innovative and disruptive Training & Talent Management
  - Operational experimentation and simulation to understand capabilities and to formulate innovative CONOPs
  - Prototyping to accelerate fielding of limited operational capabilities

Recommendations:

- AROC enforce agility to reach informed decisions for big bets.
  - Employ operational experimentation with surrogates to understand the utility of disruptive capabilities and to develop innovative CONOPs.
  - Use capability prototyping to accelerate fielding of limited operational capabilities, followed by agile development of full operational capabilities meriting full-scale development.
  - Require AOAs for all new system PORs. Examine autonomous versus manned capability solutions.

- Embrace commercial and Non-Developmental Item (NDI) technology acquisition practices for C4ISR.
  - Leverage commercial network technology and standards; employ commercial security techniques.
  - Exploit commercial space for communications and Intelligence, Surveillance, and Reconnaissance (ISR).
  - Mandate and test commercial open-system architecture (information layer) prototypes that facilitate distributed sensing, targeting, and engagement across services to enable multi-domain battle.
  - Exploit commercial as-a-service contracts process (i.e., buying outcomes).

- ASA(ALT) establish policies to:
  - Develop a high-fidelity simulation toolset for understanding RAS, IO, Cyber, AI, and human enhancement behavior in complex, realistic environments (e.g., MDB).
  - Build in dormant AI capabilities that can be dynamically activated as rules of engagement evolve.

6.3 Leader and Team Development

Findings:

- The all-volunteer force provides the U.S. a clear advantage. The value of individual Soldiers and teams drastically increase as combat capabilities proliferate to our adversaries. Battlespace reconfiguration and transparency argues for smaller, dispersed, and trained units.

- Combined and Joint capabilities migrate to lower echelons, with leaders more capable of conflict in all dimensions (physical, information, cognitive).

- “We’ve been here before,” (e.g., 1941, 1978).
  - When confronted with an existential threat, the U.S. unified and exploited our technological and entrepreneurial strengths.

  - U.S. Army recognized the value of the individual Soldier resulting in the all-volunteer force.
  - Recognition of new threats (e.g., Israeli 1973 war) motivated Army leadership to respond.

Recommendation:

- Redesign the Army for the future OE.
  - Develop and test small combat unit (company or below) prototypes led by more capable leaders leveraging more combined and joint power in a distributed, non-contiguous battle space.
  - Implement organizational design changes in the operational army based on prototype outputs.
  - Adopt talent management and diverse, advanced civil education to prepare the officer corps for conflict in all of its dimensions (physical, information, cognitive).

APPENDIX A – TERMS OF REFERENCE

SECRETARY OF THE ARMY
WASHINGTON
FEB 2 2 2017

Dr. James Tegnelia
Chairman, Army Science Board
2530 Crystal Drive, Suite 7098
Arlington, VA 22202

Dear Dr. Tegnelia:

I request the Army Science Board (ASB) conduct a study entitled "The Future Character of Warfare and Required Capabilities." The objective of the study is to assess the character of warfare in the 2030-2050 timeframe and identify solution strategies for capability development that the Army could initiate in the near-term in order to ensure ground combat forces are better prepared to achieve national objectives and sustainable political outcomes in the volatile, uncertain, complex, and ambiguous battlefields of the future.

The future operational environment will be characterized by a high potential for instability driven by the diffusion of power and technologies among rising regional states, non-state actors, and increasingly empowered individuals. Adversaries will attempt to apply emerging technologies, diverse organizations, improvised weapons, and weapons of mass destruction to increase battlefield lethality, impede access, and deny the initiative to the U.S. military, contesting it in the air, land, sea, space, and cyberspace military warfighting domains.

Global drivers like the effects of climate change, competition for resources, and shifts in demographics will all impact future strategic considerations and decisions. For instance, increasing youth populations in developing nations will create conditions for instability, especially if extremists, criminals, or other non-state actors are perceived to meet the needs and expectations of disenfranchised populations better than traditional government institutions. Absent the emergence of a global consensus with regards to managing these issues, the impact of these global drivers will add complexity to the operational environment and have the potential to undermine the ability of nation states to ensure stability, governance, and rule of law.

Therefore, the challenges of the future operational environment will require the Army of 2030-2050 to possess capabilities that achieve and maintain successful outcomes in three broad areas: (1) against nation states attempting to increase their power and influence through ways counter to the interests of the United States; (2) against non-state actors attempting to influence disenfranchised youth and gain power and influence through the co-option of economics and/or religion; and (3) engaging groups seeking access to sustenance, economic independence, and freedom from oppression.

This study will seek to examine the Army as a capability enabler and the foundation of the Joint Force in the future operational environment of 2030-2050. As such, the Army must be highly competent fighting in all the military warfighting domains, as well as employing electromagnetic spectrum activities and human/cognitive operations.

The study team's tasks shall include, but not be limited to, determining (from a technology/capability-based point of view) the following:

a. Assess and refine the projection of the world environment in 2030-2050 as it affects U.S. Army requirements and capabilities, especially related to the emerging Multi-Domain Battle concept.

b. Assess if there will be fundamental changes in the character of warfare in 2030-2050. What will these changes be, what are the drivers to these changes, and what are the implications to the U.S. Army?

c. Identify the capabilities the U.S. Army must invest in today, divest over time, and recapitalize to fight and win in the complex world of 2030-2050. Are there current U.S. Army capabilities that may not be required in 2030-2050? Are there potentially more effective and/or efficient alternative means of satisfying current requirements?

d. What policy and/or legal constraints (e.g., extending the range of cross-domain fires, conducting cyberspace operations at the tactical level, and employing lethal autonomous systems) need to be addressed in order to enable the Army to operate effectively in the 2030-2050 timeframe?

e. How will the character of war in 2030-2050 challenge American and U.S. Army ethics, morals, and values, notably when adversaries have a fundamentally different moral approach to war, violence, and enhancing human performance?

f. How should the U.S. Army prepare leaders and Soldiers for disaggregated and independent operations in degraded environments, including dense urban areas, in 2030-2050? What are the emerging technologies and capabilities that will be decisive in these environments?

To the extent possible, the study team's recommendations should not require changes in either Title 10 or the Goldwater Nichols Act, and they should recognize that the Army's Science and Technology budget is unlikely to dramatically increase over the next 10 years.

CG, TRADOC is the sponsor of this effort and will assist the study team in accessing classified information up to Top Secret and including Sensitive Compartmented Information and Special Access Programs.

A briefing and report with findings and recommendations will be provided by September 30, 2017 to the Secretary of the Army and Army Chief of Staff. The study will operate in accordance with the Federal Advisory Committee Act and Department of Defense Directive 5105.4, DoD Federal Advisory Committee Management Program. It is not anticipated that this study will need to go into any particular matters regarding the meaning of United States Code, nor will it cause any member of the study team to be placed in the position of acting as a procurement official that may constitute a conflict of interest.

Sincerely,

Robert M. Speer
Acting

APPENDIX B – STUDY TEAM MEMBERS

Michael Macedonia, Ph.D., Study Chair

Maria Mouratidis, Ph.D., Vice Chair

MG David A. Fastabend, (USA Retired)

Brig. Gen. Scott Goldstein (USAFR)

Michael Heinz

Deanne J. Idar, Ph.D.

Meg Kulungowski

Mike Molino

Sung Lee, Ph.D.

Kit Parker, Ph.D.

Joan B. Woodard, Ph.D.

BG Bob Wynn (USA, Retired)

LTC Pat Swafford, Study Manager

LTC Nik Andresky, Study Manager

Mark Swiatek, Tech Writer/Editor

APPENDIX C – TERMS, ABBREVIATIONS, AND ACRONYMS

AI	Artificial intelligence
AROC	Army Requirements Oversight Council
ASB	Army Science Board
AWE	Advanced Warfighting Experiments
C4	Command, Control, Communications, and Computer
C4ISR	Command, Control, Communications, and Computer Intelligence, Surveillance, and Reconnaissance
CDS	Capability Development Strategy
CFW	Character of Future War
COCOM	Combatant Command
CONOP	Concept of Operations
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats
CSA	Chief of Staff of the Army
DARPA	Defense Advanced Research Projects Agency
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership (and education), Personnel, and Facilities
DUA	Dense Urban Area
EW	Electronic Warfare
FAR	Federal Acquisition Regulation
FOC	Full Operational Capability
FYDP	Future Years Defense Program
GAO	Government Accounting Office
GNP	Gross National Product
ICD	Initial Capability Need
IO	Information Operations
IOC	Initial Operating Capability
IP	Intellectual Property
ISR	Intelligence, Surveillance, and Reconnaissance
JCIDS	Joint Capabilities Integration Development System
JCTD	Joint Capability Technology Demonstration
JOE	Joint Operating Environment
JUON	Joint Urgent Operational Needs
LOC	Limited Operational Capabilities

MDB	Multi-Domain Battle
MOSA	Modular Open System Architecture
MS A	Milestone A
MS B	Milestone B
MUM-T	Manned – Unmanned Teaming
NDI	Non-Development Item
OCO	Overseas Contingency Operations
OE	Operational Environment
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OODA	Observe-Orient-Decide-Act
OSD	Office of the Secretary of Defense
OTA	Other Transaction Agreement
OT&E	Operational Test and Evaluation
POM	Programming Objectives Memorandum
POR	Program of Record
PPBE	Planning, Programming, Budget, and Execution
RAS	Robotic and Autonomous Systems
R&D	Research and Development
ROE	Rules of Engagement
SES	Soldier Enhancement Study
SSE	Strategic Security Environment
TMRR	Technology Maturation and Risk Reduction
TOA	Total Obligation Authority
TRADOC	Training and Doctrine Command
TTP	Tactics, Techniques, and Procedures
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
U.S.	United States
USG	United States Government
VNSA	Violent Non-State Actor
WMD	Weapons of Mass Destruction

APPENDIX D – REFERENCES

National Intelligence Council, **Global Trends: Paradox of Progress** (January 2017)

Price Waterhouse Cooper, **The Long View: How will the Global Economic Order Change by 2050?** (February 2017)

Joint Staff J7, **Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World** (July 2016)

"**Briefing: Some Thoughts about the Security Environment, 2030-2050**" Jesse H. Ausubel, The Rockefeller University, New York 18 April 2017

UK Ministry of Defence, "**Global Strategic Trends – Out to 2045**" Fifth Edition, 30 June 2014

U.K. Ministry of Defence, "**Future Operating Environment 2035,**" 3 December 2015.

The Operational Environment, 2035-2050: The Emerging Character of Warfare, TRADOC G2 (Final Draft, June 2017)

Mad Scientist Analysis: **Robotics, Artificial Intelligence & Autonomy: Visioning Multi-Domain Warfare in 2030-2050**

"**Revisions of Reality: The Three Warfares – China's New Way of War." Laura Jackson in "Information at War: From China's Three Warfares to NATO's Narratives**." Legatum Institute, September 2015.

Milley, GEN Mark. Chief of Staff of the Army. **Speech to the AUSA Eisenhower Luncheon**, October 2016.

Mad Scientist Analysis: **The Strategic Security Environment in 2025 and Beyond**, Georgetown University and TRADOC G2 (September 2016)

Chief of Staff of the Army Strategic Studies Group Cohort IV Report: **The Character of Warfare 2030 to 2050: Technological Change, the International System, and the State** (July 2016)

Dr. Andrew Krepinevich, Center for Strategic and Budgetary Assessments, **Preserving the Balance: A U.S. Eurasia Defense Strategy** (January 2017)

Evan Braden Montgomery, Center for Strategic and Budgetary Assessments, **Reinforcing the Front Line: U.S. Defense Strategy and the Rise of China** (2017)

Mr. Eric Lindsey, Center for Strategic and Budgetary Assessments, **Beyond Coast Artillery: Cross-Domain Denial and the Army** (15 October, 2014)

Mad Scientist Analysis: **The 2050 Cyber Army**, TRADOC G2 (November 2016)

APPENDIX E – ASB APPROVED BRIEFING WITH FINDINGS AND RECOMMENDATIONS

July 2017

Army Science Board

Character of Future Warfare

What the CSA Says We Must Do

*" … we have to **place the big bets, the big bets in research and development** and **science and technology**, while simultaneously conducting legitimate and genuine **experiments** with our force designs and our doctrine.*

*… **every assumption** we hold, every claim, every assertion, every single one of them **must be challenged**. … Those of us, or those **nation-states that stubbornly cling to the past will lose**. They will lose that war, and they will lose it in a big way.*

*… we should **think of nothing in the past as sacred**, except the concept of victory."*

GEN MARK MILLEY, CSA AT AUSA
"CHANGING NATURE OF WAR WON'T CHANGE OUR PURPOSE", OCT. 1, 2016

Study Overview

- **Terms of Reference (TOR)**
  - **Sponsor:** CG, TRADOC
  - **Purpose:** assess the character of warfare in the 2030-2050 timeframe and **identify solution strategies for capability development** that the Army could initiate in the near-term
  - **Schedule: January-July 2017**
  - **Critical Tasks:**
    - Assess and refine projected future world environment as it affects Army requirements
    - Assess and identify if there will be fundamental changes in CFW and impact on Army
    - Identify Army capabilities in which to invest and from which to disinvest

Character of War Defined

Nature of War *"…threat of violence, as an extension of politics, to* ***compel the enemy to our will*** *within the fog, friction and chance of combat—is* ***immutable****."*

Character of War *"….or its expression and form,* ***changes due to unique geo-political, social, demographic, economic and technological developments interacting****, often unevenly, over time…"*

GEN MARK MILLEY, CSA AT AUSA
"CHANGING NATURE OF WAR WON'T CHANGE OUR PURPOSE", OCT. 1, 2016

Team Members and Visits

Team

- Dr. Michael Macedonia (Study Lead)
- Dr. Maria Mouratidis (Vice Chair)
- LTC Pat Swafford (Study Manager)
- LTC Nik Andresky (Study Manager)
- David Fastabend
- BG (USAF) Scott Goldstein
- Michael Heinz
- Dr. Deanne J. Idar
- Meg Kulungowski
- Mike Molino
- Dr. Sung Lee
- LTC Kit Parker, Ph.D.
- Dr. Joan B. Woodard
- BG (Ret) Bob Wynn

Red Team

- GEN (Ret) Dave Maddox
- Dr. Leonard Braverman

Visits and Briefings

- DoD / Government Organizations:
  - Federal Government: ODNI, Comptroller General of the U.S. (GAO)
  - OSD/Joint: DTRA, DARPA
  - Army: DAMO-SS, USMA (MWI), FCOE, MCOE, USAPAC, G8 FDM Aviation
- FFRDCs/Academe/Non-Federal: RAND, FED RES Bank (NY); Rockefeller University
- Industry: IBM (Watson), Burston Marsteller, Teal Group, Microsoft Research, SpaceX
- Exhaustive number of studies on the future and the future of war

Army Science Board 5

Outline

- Strategic security environment complexity: **Increasing**
- Adversary ability to exploit technology: **Increasing**
- Army operational challenges: **Increasing**
- Army big bet options: **Increasing**

CONSTRAINED BY

- Army budget to fund big bets: **Stagnant or Decreasing**
- Asymmetric policies and laws to exploit big bets: **Stagnant**
- Formal acquisition timeliness to field big bets: **Stagnant or Worse**

THEREFORE ARMY NEEDS

- Innovative CONOPs & integration to gain overmatch from Big Bets
  - Prioritize MUM-T investments across successive POMs
  - Increase lethality
  - Embrace commercial & NDI technology acquisition practices for C4ISR
  - Redesign the Army for the future operational environment

Army Science Board 6

Study Logic: Character of Future Warfare

Assessment Methodology
- Analyzed sources using 'From–To' approach
- Reviewed & extracted common threads

Env	From	To
SSE	Ready to fight a near-peer adversary (15 years ago)	Significantly degraded readiness vis a vis near-peers
SSE	Unipolar environment	Multipolar environment
SSE	Instability the Exception	"instability is the new normal"
SSE	Developing mega-city	Extensive mega-city urbanization
OE	Communication linkages controllable by nation states	Operational commercial "transparency" increasing
OE	U.S. monopoly on precision	Precision and lethality of systems accelerating & proliferating
OE	No Artificial Intelligence	Artificial Intelligence advancing
OE	Air, Maritime, Space Supremacy	Tactical Parity; challenged in all domains
OE	Army masses in static, protected areas	Probability of detection and engagement very high everywhere

Army Science Board 7

Reviewed & Assessed Many Studies (and Assumptions)

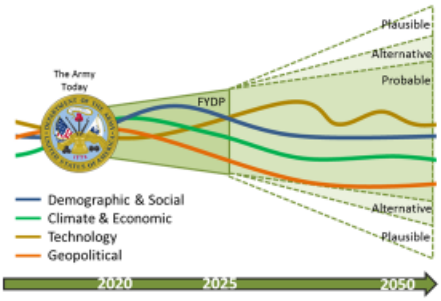
- UK MoD
- National Intelligence Center
- Office of Net Assessment
- Joint Operating Environment
- TRADOC SSE Mad Scientist
- RAND
- CSA SSG
  - Year 1
  - Year 2
- CSA – Oct. 2016
  - AUSA article & briefing
- Draft ASP narrative

Army Science Board 8

Trends and Implications: Strategic Security Environment (SSE) in 2030-2050

Demographics & Social
- Population implosions & explosions drive migration
- Accelerating Dense Urban Areas
- Developed, aging countries: military recruiting difficult
- Non-Developed countries: large bulge of disenfranchised youth challenges governance; available for military service

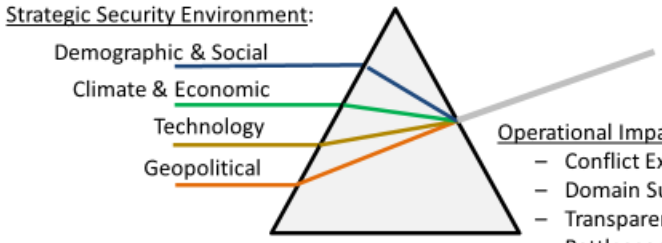
Climate & Economic
- World trade continues to intertwine
- Corporations increasingly international with a greater impact on geopolitics
- Climate change accelerates migration & instability



Technology
- Technology available & affordable on open market; technology flow from DoD R&D reverses
- Weapon precision & lethality proliferating and accelerating; U.S. tactical supremacy disappearing
- WMD proliferation continues; U.S. escalation advantage erodes
- Connectivity enables decisive misinformation campaigns (e.g., Ukraine & Crimea)
- Human Enhancement offers Soldier superiority to those willing to use it
- AI compresses decision space at every level: strategic/operational/tactical

Geopolitical
- Shifts in global power: U.S. "superpower" supremacy gap narrows or disappears
- Treaties and alliances are changing; economics remain a major driving factor
- U.S. threat: **peer, near-peer; violent non-state actors**

Trends and Implications: Operational Environment (OE) in 2030-2050

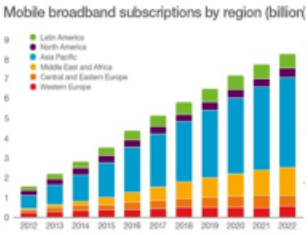


Operational Impacts:
- Conflict Extends to Cognitive Domain
- Domain Supremacy Contested
- Transparent War
- Battlespace Reconfiguration
- Contested Expeditionary Ops

Operational Impact: Conflict Extends to Cognitive Dimension

FROM	TO
Competition for **will** primarily kinetic	Competition for **will** increasingly non-kinetic and continuous

'The very "rules of war" have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.' **- Gerasimov**



- Western cultures are ill-positioned for warfare in the information & cognitive dimensions of conflict: we face daunting, asymmetrical legal & institutional constraints.
- Armies must leverage multiagency and multinational power to win the emerging contest for **will**.
- Adversaries have posited aggressive doctrines ("New Generation Warfare"; "Three Warfares") to do this.
- We lack effective cyber/IO CONOPs to overmatch or counter adversary influence operations.
- Kinetic/cyber/IO operations are stove-piped both institutionally and conceptually.

Operational Impact: Domain Supremacy Contested

FROM	TO
Supremacy in all domains	More lethal and contested in all domains

- Tactical engagements are
  - compressed in time
  - extended in space
  - more lethal
  - connected across domains (air/land/sea/space/cyber)
  - interactive across the conflict dimensions (physical/informational/cognitive)

- Tactical engagements in physical dimension favor the defense; information dimension will be continuous and favors the offense. Protracted operations more likely.
- MUM-T required to survive more lethal battlespace.
- Land forces must leverage UAS/RAS to regain local air dominance and enable maneuver.
- Innovative CONOPs required to leverage disruptive technologies into advanced combined arms capabilities.
- Current Army capability development process suboptimal to enable advanced combined arms capabilities development.

Operational Impact: Transparent War

FROM	TO
Limited, stove-piped, military C4ISR	Continuous & pervasive commercial C4ISR

- Network:
  - 50 billion devices connected to global Fiber/RF/SATCOM nodes
  - Dense EM and Cyber environments, commercial communications
- Sensor:
  - Explosive growth of **commercial** ISR from satellites, drones and IOT
  - Sophisticated ISR available to DoD, near-peer & violent non-state actors alike
- Operational transparency increasing and beyond state control.
- Relentless and continuous fight for connectivity via IO, cyber and EW.
- C2 capabilities augmented at lower echelons.
- Sensor, processing, and engagement speeds shift decision space increasingly to machines via AI.
- Increased combat support effects from CONUS to dispersed forward forces.

Operational Impact: Battlespace Reconfiguration

FROM	TO
Maneuver primarily in open terrain & contiguous areas of operation	Maneuver extends to Dense Urban Areas & dispersed, noncontiguous areas of operation

- Conflict in Dense Urban Operations increases, as urban areas expand and all competitors seek:
  - Concealment from ubiquitous sensors
  - Overhead cover from peer-capable engagement systems
- Cities become a necessity – even an opportunity -- for foraging, e.g., water, energy, 3D printing materials, communications, transportation assets
- "Pulse logistics" v. "Continuous logistics"
- U.S. CONOPs that "destroy to save" are no longer acceptable; non-combatants planning may shape and define the outcome
- IPB/SA to include culture, history and patterns of life
- Units will disperse and disaggregate to frustrate detection and engagement; wide area control less feasible and battlespace non-contiguous

- Combined and Joint capabilities migrate to lower echelons
- Units must mass effects vice forces: range overmatch at a premium for both sensors and weapons
- Dispersed forces constantly on the move need beyond line of sight connectivity
- Comms across a non-contiguous battlespace far from assured; advanced Mission Command must enable subordinate recognition/action when mission should change

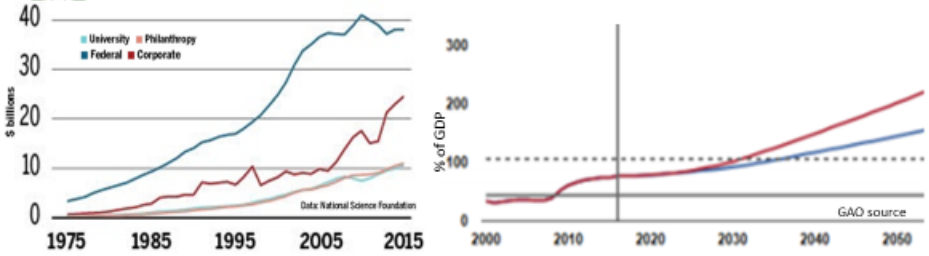
Operational Impact: Contested Expeditionary Ops

FROM	TO
Power projection "at will"	Continuously contested from alert to employment

- Constant surveillance - Ubiquitous sensors & networks in use from home station to employment - adversary constantly aware
- Deploying forces continuously at risk of **lethal engagement** in multiple domains
- Robust A2/AD regimes restricts expeditionary maneuver into expected areas of entry
- Peer competitors may conduct expeditionary operations as well (e.g., Djibouti)
- Requires mass from fires and maneuver of dispersed, covert, concentrated, small unit forces to achieve surprise
- Retain and leverage forward presence
- Land forces must fight into and under an enemy A2/AD regime

Illustrative A2/AD environment

Three Key Constraints



How to enable capability agility given **fiscal constraints** & future uncertainties?

- **Only a few** "big bets" on future disruptive capabilities can be made within fiscal constraints.

How to offset **asymmetries in acquisition**?

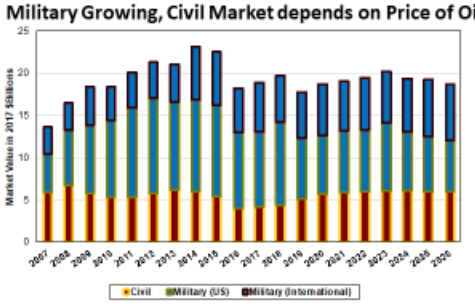
- For any new major POR, **2030 is only one acquisition cycle away** for Initial Operating Capability; 2050 is just one procurement buyout away for that system.
- Army "tribes" inhibit collaborative exploitation of disruptive technologies and capabilities (e.g., RAS for Fires), and limits creative space.

How to hedge against **legal & cultural asymmetries** in use of disruptive capabilities?

- **Adversaries have no compunction** to use lethal autonomy, offensive cyber, information distortion, drugs, genetics and civilian casualties.

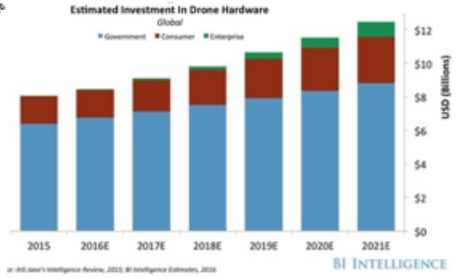
An Example of Fiscal Constraints: UAVs versus Manned Rotorcraft

U.S. Military Rotorcraft Market Falling; International Military Growing, Civil Market depends on Price of Oil



Army only significant buyer in the rotorcraft capital-intensive industry; creates significant fiscal/technical risk to the Army.

Commercial and Government drone investments just started up the S-curve.



Capability Development Strategy

- Objectives:
  - (1) Gain insights into operational utility of a proposed capability
  - (2) Evaluate concepts to inform CONOPs that best exploit the capabilities
  - (3) Accelerate fielding of limited operational capability prior to formal acquisition of Full Operational Capability
- Use operational experimentation and simulation (AWE-like, but single capability focused) for objectives (1) and (2)
  - ***Functional*** experiments using ***physical surrogates***
  - Limited set of realistic and stressing scenarios and conditions
  - Two teams (control & capability enhanced) with iterative learning
  - Simulation drives the experiment and allows extrapolation to other scenarios and conditions
- Use Army tech demonstration prototyping (JCTD-like) for objective (3)
  - Purpose built ***physical*** prototype
  - Residual assets may be fielded with ***limited operational capability***
  - Formal acquisition initiated at MS B for systems that prove value

Findings: A Call to Action

- Changes to the Character of Future Warfare (CFW) are inexorable and accelerating, which make maintaining overmatch, without appropriate response, more difficult. Our adversaries are reducing, if not eliminating, our overmatch.
- Easy global access to emerging technologies (Robotic Autonomous Systems (RAS), Cyber, Influence Operations (IO), Artificial Intelligence (AI), and human enhancements) are leveling the playing field, and increasing lethality.
- "We've been here before," (e.g., 1941, 1978):
  - When confronted with an existential threat, the U.S. unified & exploited our technological & entrepreneurial strengths
  - U.S. Army recognized the value of the individual Soldier resulting in the all-volunteer force
  - Recognition of new threats (e.g. Israeli 1973 war) motivated Army leadership to respond
- Even without Allies' recognition of an existential threat, the U.S. will have to make the preponderance of the Allied national security investment.
- Army leadership has recognized the impact of the Ukrainian war yet has not communicated the solutions for our Army to respond to this type threat.
- The Army has underinvested in new, fielded munitions since mid 80's.

Changes to the CFW create opportunities; exploiting Big Bets will provide overmatch

Findings: A Call to Action

- Army lacks Capability Development Strategy across Centers of Excellence to exploit:
  - Innovative and disruptive Training & Talent Management
  - Operational experimentation & simulation to understand capabilities and to formulate innovative CONOPs
  - Prototyping to accelerate fielding of limited operational capabilities
- The all-volunteer force provides the U.S. a clear advantage. The value of individual Soldiers and teams drastically increase as combat capabilities proliferate to our adversaries. Battlespace reconfiguration and transparency argues for smaller, dispersed & trained units.
- Combined and Joint capabilities migrate to lower echelons, with leaders more capable for conflict in all dimensions (physical, information, cognitive).
- The Army has no plan to defeat enemy integrated air defense. Non-developmental Unmanned Aircraft System (UAS), coupled with innovative CONOPs, appears a viable approach to mitigate Integrated Air Defense (IAD) challenge.
- The introduction of ground and air robotic combat vehicles changes both the lethality and survivability parameters.

Recommendations #1: Big Bets for Enhanced Battle Outcomes

1. **Prioritize MUM-T investments across successive POMs**
   - Focus on ground MUM-T; it is a unique Army capability and will not occur without Army investment
   - Leverage other services for air MUM-T
   - Exploit commercial AI development and adapt for Army unique applications
2. **Increase lethality**
   - New payloads and longer range fires
   - Area effect munitions
   - Kinetic energy missiles
3. **Embrace commercial & Non-Developmental Item (NDI) technology acquisition practices for C4ISR**
   - Leverage commercial network technology & standards; employ commercial security techniques
   - Exploit commercial space for communications and Intelligence, Surveillance and Reconnaissance (ISR)
   - Mandate & test commercial open system architecture (information layer) prototypes that facilitates distributed sensing, targeting and engagement across services to enable multi-domain battle
   - Exploit commercial as-a-service contracts process; buying outcomes
4. **Redesign the Army for the future operational environment**
   - Develop and test small combat unit (company or below) prototypes led by more capable leaders, leveraging more Combined and Joint power in distributed, non-contiguous battle space
   - Implement organizational design changes in the operational army based on prototype outputs
   - Adopt talent management and diverse, advanced civil education to prepare the officer corps for conflict in all dimensions (physical, information, cognitive)

Recommendation #2: Invest & Divest

Invest

- MUM-T armed ground robotic vehicles
- Commercial network capability for Army participation in Multi-Domain Battle (MDB)
- Lethality
- Education, training, cadre, facilities and infrastructure to enhance overmatch in Soldier (enlisted, warrant officer and officer) and team performance
- Cyber, Influence Operations and EW as Army tactical weapon systems
- Leverage DARPA innovation (e.g., Cognitive EW, Swarming UAVs & Offset, Squad-X)

Divestment Strategies

The Army should develop divestment strategies for systems that no longer meet current and future threats to harvest and redirect funds, for example:

- Army developed, unique networks that do not meet the needs of MDB
- Enhancements to armored combat vehicles that add weight
- Manned aviation platforms and their enhancements not required in a MUM-T environment

Recommendation #3: Overcome Capability Development Constraints

- AROC enforce agility to reach informed decisions for big bets
  - Employ operational experimentation with surrogates to understand the utility of disruptive capabilities and to develop innovative CONOPs.
  - Use capability prototyping to accelerate fielding of limited operational capabilities, followed by agile development of full operational capabilities meriting full scale development.
  - Require AOAs for all new system PORs examine autonomous vs. manned capability solutions.

- ASA(ALT) establish policies to:
  - Develop a high fidelity simulation toolset for understanding RAS, IO, Cyber, AI and human enhancement behavior in complex, realistic environments (e.g., MDB).
  - Build in dormant AI capabilities that can be dynamically activated as rules of engagement evolve.